TAB 13

1 of 2 DOCUMENTS

Federal News Service

February 6, 2006 Monday

SECTION: PRESS CONFERENCE OR SPEECH

LENGTH: 39300 words

HEADLINE: AFTERNOON SESSION OF A HEARING OF THE SENATE JUDICIARY COMMITTEE

SUBJECT: "WARTIME EXECUTIVE POWER AND THE NATIONAL SECURITY AGENCY'S SURVEILLANCE AUTHORITY"

CHAIRED BY: SENATOR ARLEN SPECTER (R-PA)

WITNESS: U.S. ATTORNEY GENERAL ALBERTO GONZALES

LOCATION: 216 HART SENATE OFFICE BUILDING, WASHINGTON, D.C.

BODY:

SEN. SPECTER: (Sounds gavel.) It's 1:45. The committee prides itself on being prompt. And we thank you, Mr. Attorney General, for being prompt coming back.

I think the hearings have been very productive. And we have had full attendance, almost full attendance. And I think the other senators who could not be here earlier -- it is unusual to have a Monday morning session for the United States Senate. And we have done that because this committee has been so busy. And we have asbestos reform legislation which Senator Leahy and I are co-sponsoring, which is coming to the floor later today, and we've had a full platter with the confirmation of Justice Alito. And we wanted to have this hearing at an early date, and this was the earliest we could do, which, given the intervening holidays after the program was announced back on December 16th, we have proceeded.

We anticipated a full day of hearings and at least two rounds, and it's apparent to me at this point that we're not going to be able to finish today within a reasonable time. Senator Feingold's nodding in the affirmative. That's the first time I've gotten him to nod in the affirmative today. So you see, we're making some progress.

But I do believe there will be a full second round. And we don't function too well into the evening. If we have to, we do, but it's difficult for the witness. And I've conferred with the attorney general, who has graciously consented to come back on a second day.

So we will proceed through until about 5:00 this afternoon, and then we will schedule another day. By that time, everybody will have had a full -- a first round, and it will give us time to digest what we have heard, and we will proceed on a second day.

Senator Feingold, you're recognized.

SEN. RUSSELL FEINGOLD (D-WI): Good afternoon, Mr. Attorney General.

Mr. Chairman, let me say of course we have a disagreement, Mr. Chairman, about whether this witness should have been sworn, and that is a serious disagreement. But let me nod in an affirmative way about your Pittsburgh Steelers, first of all. (Laughter.)

SEN. SPECTER: (Chuckles.)

SEN. FEINGOLD: Secondly, let me say --

SEN. SPECTER: Green Bay --

SEN. FEINGOLD: Green Bay will be back, Mr. Chairman.

SEN. SPECTER: With Green Bay out of it, why not root for the Steelers, Senator Feingold?

SEN. LEAHY: That's why we didn't have the hearing last night.

SEN. FEINGOLD: Well, I understood that. I was curious about that.

Mr. Chairman --

SEN. SPECTER: Re-set the clock at 10 minutes. (Laughter.)

SEN. FEINGOLD: (Laughs.)

SEN. SPECTER: I was only kidding. (Laughter.)

SEN. FEINGOLD: Let me also say, Mr. Chairman, despite our disagreement about the swearing-in issue, that I praise you for your candor and your leadership on this issue and for holding this hearing and the other hearings you may be holding.

I also want to compliment some of my colleagues on the other side of the aisle for their candor on this issue already publicly. People like Senator DeWine, Senator Graham, Senator Brownback. Maybe they don't want me to mention their names, but the fact is they have publicly disputed this fantasy version of the justification of this based on the Afghanistan resolution. It is a fantasy version that no senator, I think, can actually believe that we authorized this wiretapping.

So the fact is this can and should be a bipartisan issue. I see real promise for this being a bipartisan issue, and it should be. But the problem here is that the -- what the administration has said is that when it comes to national security, the problem is that the Democrats have a pre-9/11 view of the world. But let me tell you what I think the problem is. The real problem is that the president seems to have a pre-1776 view of the world. That's the problem here. All of us are committed to defeating the terrorists who threaten our country, Mr. Attorney General. It is without a doubt our top priority. In fact, I just want to read again what you said. "As the president has said, if you talking with al Qaeda, we want to know what you're saying." Absolutely right. No one in this committee, I think no one in this body believes anything other than that, and I want to state it as firmly as I can.

But I believe that we can and must do that without violating the Constitution or jeopardizing the freedoms on which this country was founded. Our forefathers fought a revolution -- a revolution to be free from rulers who put themselves above the law. And I got to say, Mr. Chairman, I think this administration has been violating the law and is misleading the American people to try to justify it.

This hearing is not just a hearing about future, possible solutions. That is fine to be part of the answer and part of the hearing. This hearing, Mr. Chairman, is also an inquiry into possible wrongdoing.

Mr. Attorney General, there have already been a few mentions today of your testimony in January of '05 -- your confirmation hearing. I'm going to ask you a few quick simple and factual questions, but I want to make it clear that I don't think this hearing is about our exchange or about me or what you said to me in particular. I am concerned about your testimony at that time because I do believe it was materially misleading. But I am even more concerned about the credibility of your administration, and I'm even more concerned than that about the respect for the rule of law in this country. So that is the spirit of my questions.

Mr. Attorney General, you served as White House Counsel from January 2001 until you became attorney general in 2005. On January 6th, 2005, you had a confirmation hearing for the attorney general position before this committee. Mr. Attorney General, you testified under oath at that hearing, didn't you?

ATTY GEN. GONZALES: Yes, sir.

SEN. FEINGOLD: And sir, I don't mean to belabor the point, but just so the record is clear, do you or anyone in the administration ask Chairman Specter or his staff that you not be put under oath today?

ATTY GEN. GONZALES: Senator, I've already indicated for the record the chairman asked my views about being sworn in, and I said I had no objection.

SEN. FEINGOLD: But did anyone -- you or anyone in the administration ask the chairman to not have you sworn?

ATTY GEN. GONZALES: Sir, not to my knowledge.

SEN. FEINGOLD: Okay.

SEN. SPECTER: The answer's no.

SEN. FEINGOLD: At the time -- that's fine.

At the time you testified in January of '05, you were fully aware of the NSA program, were you not?

ATTY GEN. GONZALES: Yes, sir.

SEN. FEINGOLD: You were also fully aware at the time you testified that the Justice Department had issued a legal justification for the program. Isn't that right?

ATTY GEN. GONZALES: Yes, I had the legal analysis performed by the Department of Justice.

SEN. FEINGOLD: And you, as White House counsel, agreed with that legal analysis, didn't you?

ATTY GEN. GONZALES: I agree with the legal analysis, yes.

SEN. FEINGOLD: And you had signed off on the program, right?

ATTY GEN. GONZALES: Yes, I do believe the president -- I did believe at the time the president has the authority to authorize these kind of --

SEN. FEINGOLD: And you had signed off on that legal opinion.

And yet when I specifically asked you at the January 2005 hearing whether, in your opinion, the president can authorize warrantless surveillance, notwithstanding the foreign intelligence statutes of this country, you didn't tell us yes. Why not? Why not?

ATTY GEN. GONZALES: Sir, I believe your question -- the hypothetical you pose -- and I do consider a

hypothetical -- which is whether or not -- had the president authorized activity in -- specific electronic surveillance in violation of the laws. And I have tried to make clear today that in the legal analysis in the white paper, the position of the administration is that we -- the president has authorized electronic surveillance in a manner that's totally consistent -- not in violation, not in -- not overriding provisions of FISA, but totally consistent with FISA.

SEN. FEINGOLD: Well, Mr. -- General, certainly it was not a hypothetical, as we now know.

ATTY GEN. GONZALES: Your -- Senator, your question was whether or not the president had authorized certain conduct in violation of law. That was a hypothetical.

SEN. FEINGOLD: My question was whether the president could have authorized this kind of wiretapping.

ATTY GEN. GONZALES: In violation of the criminal statutes. And our position is and has been -- is that no, this is not in violation of the criminal statutes. FISA cannot --

SEN. FEINGOLD: You said that was your -- you said the question was merely hypothetical, and that -- look, this is what you said: "It's not the policy or the agenda of this president to authorize actions that would be in contravention of our criminal statutes." And when you said that, you knew about this program. In fact, you just told me that you had approved it and you were aware of the legal analysis to justify it.

You wanted this committee and the American people to think that this kind of program was not going on, but it was, and you knew that. And I think that's unacceptable.

ATTY GEN. GONZALES: Senator -- Senator, your question was whether or not the president had authorized conduct in violation of law, and I've laid out --

SEN. FEINGOLD: The question was whether the --

ATTY GEN. GONZALES: I have --

SEN. FEINGOLD: -- Mr. Attorney General, my question was whether the president would have the power to do that.

ATTY GEN. GONZALES: And, Senator, the president has not authorized conduct in violation of our criminal statutes. We've laid out a 42-page analysis of our legal position here. The authority the president has exercised are totally consistent with the criminal provision -- the primary criminal provision in FISA, Section 109.

SEN. FEINGOLD: I've heard all your arguments, but I want to get back to your testimony, which, frankly, Mr. Attorney General, anybody that reads it basically realizes you were misleading this committee. You could have answered the question truthfully. You could have told the committee that, yes, in your opinion, the president has that authority. By simply saying the truth that you believe the president has the power to wiretap Americans without a warrant would not have exposed any classified information.

And my question wasn't whether such illegal wiretapping was going on. Like almost everyone in Congress, I didn't know, of course, about the program then. It wasn't even about whether the administration believed that the president has this authority. It was a question about your view of the law -- about your view of the law --

ATTY GEN. GONZALES: Senator --

SEN. FEINGOLD: -- during the confirmation on your nomination to be attorney general. So, of course, if you had told the truth, maybe that would have jeopardized your nomination. You wanted to be confirmed, and so you let a misleading statement about one of the central issues of your confirmation, your view of executive power, stay on the record until The New York Times revealed the program.

ATTY GEN. GONZALES: Senator, I've told the truth then. I'm telling the truth now. You asked about a hypothetical situation of the president of the United States authorizing electronic surveillance in violation of our criminal statutes. That has not occurred.

SEN. FEINGOLD: Mr. Chairman, I think the witness has taken mincing words to a new high, and there it is no question in my mind that when you answered the question that was a hypothetical, you knew it was not a hypothetical, and you were under oath at the time.

Let me switch to some other misrepresentations.

SEN. SPECTER: Wait a minute. Did you care to answer that, Attorney General Gonzales?

ATTY GEN. GONZALES: Senator, as I've stated before, what I said was the truth then. It is the truth today. The president of the United States has not authorized electronic surveillance in violation of our criminal statutes. We have laid out in great detail our position that the activities are totally consistent with the criminal statute.

SEN. FEINGOLD: All you had to do, Mr. Attorney General, was indicate that it was view that it was legal. That was what my question was. I would have disagreed with your conclusion. But that's not what you said, and you referred to this as merely a hypothetical.

Mr. Attorney General, the administration officials have been very misleading in their claims in justifying the spying program. To make matters worse, last week in the State of the Union, the president repeated some of these claims. For one thing, the president said that his predecessors have used the same constitutional authority that he has. Isn't it true that the Supreme Court first found that phone conversations are protected by the Fourth Amendment in the 1967 Katz case?

ATTY GEN. GONZALES: Yes. In the 1967 Katz case, the Supreme Court did find that telephone conversations would be -- are covered by the Fourth Amendment.

SEN. FEINGOLD: So when the Justice Department points to Presidents Wilson and Roosevelt's actions, those are really irrelevant, aren't they?

ATTY GEN. GONZALES: Absolutely not, Senator. I think that they're important in showing that presidents have relied upon their constitutional authority to engage in warrantless surveillance of the enemy during a time of war. Feb 06, 2006 16:43 ET .EOF

The fact that the Fourth Amendment may apply doesn't mean that a warrant is necessarily required in every case, as you know. There is a jurisprudence of the Supreme Court regarding special needs normally in the national security context, outside of the ordinary criminal law context, where because of the circumstances, searches without warrants would be justified.

SEN. FEINGOLD: Mr. Chairman, my time's up. I'll continue this line of questioning later.

SEN. SPECTER: Thank you very much, Senator Feingold.

Senator Graham.

SEN. LINDSEY GRAHAM (R-SC): Thank you, Mr. Chairman. I would like to congratulate you also for having these hearings. I think what we're talking about is incredibly important for the country in terms of the future conduct of wars and how we relate constitutionally to each other, and personally how we relate. I find your testimony honest, straightforward; your legal reasoning is well articulated; I don't agree with it all.

About hiding something about this program, is it not true that the Congress has been briefed extensively, at least a

small group of congressmen and senators, about this program?

ATTY GEN. GONZALES: Senator, I have not been present, as I've testified before, at all of the briefings, but in the briefings that I have been present, the briefings were extensive, the briefings were detailed. Members who were present at the briefing were given an opportunity to ask questions, to voice concerns.

SEN. GRAHAM: And if any member of this body believed that you've done something illegal, they could put in legislation to terminate this program, couldn't they? Isn't that our power?

ATTY GEN. GONZALES: Certainly, Senator, it --

SEN. GRAHAM: Well, I would think if you believed that our president was breaking the law, you'd have the courage of your convictions and you'd bring -- you'd stop funding for it.

Now, it seems to me there's two ways we can do this. We can argue what the law. We can argue if it was broken. We can play a political dance of shirts versus skins. Or we can find consensus as to what the law should be. And I associate myself with Senator DeWine as to what I think it should be. In a dangerous and difficult time for our country, I chose inquiry versus inquisition, collaboration versus conflict.

To me, there's two big things that this Congress faces and this president faces. In all honesty, Mr. Attorney General, the statutory force resolution argument that you're making is very dangerous in terms of its application for the future, because if you overly interpret the force resolution -- and I'll be the first to say when I voted for it, I never envisioned that I was giving to this president or any other president the ability to go around FISA carte blanche. And you're right, it is not my -- my intent is the letter of the resolution. What I'm saying is that if you came back next time, or the next president came back to this body, there would be a memory bank established here. And I would suggest to you, Mr. Attorney General, it would be harder for the next president to get a force resolution if we take this too far, and the exceptions may be a mile long.

Do you share my concern?

ATTY GEN. GONZALES: I understand your concern, Senator.

SEN. GRAHAM: Thank you. And that's -- I appreciate that. So that's just a comment about the practical application of where we could go one day if we overinterpret.

Because the offer's on the table. Let's make sure we have the same understanding. Because if we have the same understanding between the executive, the legislative and the judicial branch, our enemy is weaker and we're stronger.

Now to the inherent authority argument. Taken to its logical conclusion, it concerns me that it could basically neuter the Congress and weaken the courts, and I'd like to focus a minute on the inherent authority of the president during a time of war concept.

Let me give you a hypothetical, and you can answer it if you choose to, and I understand if you won't. There's a detainee in our charge, an enemy prisoner, a high-value target. We reasonably believe that this person possesses information that could save millions or thousands of American lives. The president, as the commander in chief, tells the military authorities in charge, "You have my permission, my authority, and I'm ordering you, do all things necessary, and these five things I'm authorizing. Do it because I'm commander in chief and we got to protect the country."

There's a pre-existing statute on the book passed by the Congress called the Uniform Code of Military Justice, and it tells our troops that if you have a prisoner in your charge, you're not to do these things, and they're the same five things. What do we do?

ATTY GEN. GONZALES: Well, of course, Senator, the president has already said that we're not going to engage

in torture. He has made that -- that is a categorical statement by the president.

As to whether or not the statute that you referred to would be constitutional, these kinds of questions are very, very difficult. One could make the argument, for example, that the provision in the Constitution that talks about Congress under Section 8 of Article I giving Congress the specific authority to make rules regarding captures -- that that would give Congress the authority to legislate in this area. Now, there is some disagreement amongst scholars about --

SEN. GRAHAM: And I tell you this -- it's talking about ships. It's not talking about people. But it's clear to me that the Congress has the authority to regulate the military, to fund the military, and the Uniform Code of Military Justice is a statutory scheme providing guidance, regulation and punishment to the military that the Congress passes.

ATTY GEN. GONZALES: That would -- I think most scholars would say that fall under -- that's the clause in Section 8 of Article I giving the Congress the authority to pass rules regarding government and regulation of the armed forces.

SEN. GRAHAM: And I would agree with those scholars. And the point I'm trying to say is that we can tell our military, "Don't you do this to a detainee." And you as commander in chief can tell the military, "We got to win the war. We got to protect ourselves." Now what I'm trying to say is that the -- I'm worried about the person in the middle here, because if we adopted the reasoning of the Bybee memo -- has been repudiated, appropriately -- the point I was trying to make at your confirmation hearing is that the legal reasoning used in determining what torture would be under the convention of torture or the torture statute not only was strained, that made me feel uncomfortable; it violated an existing body of law that was already on the books called the Uniform Code of Military Justice. If a military member had engaged in the conduct outlined by the Bybee memo, they could have been prosecuted for abusing a detainee because it's a crime in the military, Mr. Attorney General, for a guard to slap a prisoner, much less have something short of major organ failure.

This is really a big deal for the people fighting the war. And if you take your inherent-authority argument too far, then I am really concerned that there is no check and balance. And when the nation's at war, I would argue, Mr. Attorney General, you need checks and balances more than ever, because within the law, we put a whole group of people in jail who just looked like the enemy.

ATTY GEN. GONZALES: Senator, if I could just respond. I'm not -- maybe I haven't been as precise with my words as I might have been. I don't think I've talked about inherent exclusive authority, I've talked about inherent authority under the Constitution in the commander in chief. Congress, of course, and I've said in response to other questions, they have a constitutional role to play also during a time of war.

SEN. GRAHAM: We coexist.

Now, can I get to the FISA statute in two minutes here? And Mr. -- I hope we do have another round, because this is very important. I'm not here to accuse anyone of breaking the law; I want to create law that will help people fighting the war know what they can and can't do.

The FISA statute, if you look at the legislative language, they made a conscious decision back in 1978 to resolve this two-lane debate. There's two lanes you can go down as commander in chief. You can act with the Congress and you can have inherent authority as commander in chief. The FISA statute said basically this is the exclusive means to conduct foreign surveillance where American citizens are involved, and the Congress, seems to me, gave you a one-lane highway, not a two-lane highway. They took the inherent- authority argument, they thought about it, they debated it, and they passed a statute, if you look at the legislative language, saying this shall be the exclusive means. And it's different than 1401.

So I guess what I'm saying, Mr. Attorney General, if I buy our argument about FISA, I can't think of a reason you wouldn't have the ability, if you chose to, to set aside the statute on torture if you believed it impeded the war effort.

ATTY GEN. GONZALES: Well, Senator, whether or not we set aside a statute, of course, is not --

SEN. GRAHAM: That inherent authority sets aside the statute.

ATTY GEN. GONZALES: That's not what we're talking about here. We don't need to get to that tough question.

SEN. GRAHAM: If you don't buy the force resolution argument, if we somehow magically took that off the table, that's all you're left with, is the inherent authority. And Congress could tomorrow change that resolution, and that's dangerous for the country if we get in a political fight over that.

All I'm saying is the inherent-authority argument in its application, to me, seems to have no boundaries when it comes to executive decisions in a time of war. It deals the Congress out, it deals the courts out. And Mr. Attorney General, there is a better way, and on our next round of questioning, we will talk about that better way.

ATTY GEN. GONZALES: Sir, can I simply make one quick response?

SEN. GRAHAM: You may. You may respond, Attorney General.

ATTY GEN. GONZALES: Well, the fact that the president, again, may have inherent authority doesn't mean that Congress has no authority in a particular area. And we look at the words of the Constitution and there are clear grants of authority to the Congress in a time of war. And so if you're talking about competing constitutional interests, that's when you get into sort of the third part of the Jackson analysis.

SEN. GRAHAM: That's where we're at right now.

ATTY GEN. GONZALES: I don't believe that's where we're at right now.

SEN. GRAHAM: That's where you're at with me. (Laughs.)

ATTY GEN. GONZALES: Sir, even under the third part of the Jackson analysis -- again, I haven't done the detailed work that obviously these kinds of questions require; these are tough questions, but I believe that the president does have the authority under the Constitution.

SEN. SPECTER: Thank you, Senator Graham. Senator Schumer.

SEN. CHARLES SCHUMER (D-NY): Thank you, Mr. Chairman. And General Gonzales, I just want to make a couple of points that are important to keep in mind as we ask you questions.

First, we all support a strong, robust and vigorous national- security program. Like everyone else in this room, I want the president to have all the legal tools he needs as we work together to keep our nation safe and free, including wiretapping. And I appreciate the difficult job you and the president have, balancing security and liberty. That is not an easy one.

But I firmly believe that we can have both security and rule of law. And I'm sure you agree with that, General Gonzales, don't you?

ATTY GEN. GONZALES: Yes, Senator.

SEN. SCHUMER: And that's what distinguishes us from so many other nations, including our enemies. Is that correct?

ATTY GEN. GONZALES: That is correct.

SEN. SCHUMER: Okay. Now, the first job of government is to protect our security, and everyone on this

committee supports that. But another important job of government is to enforce the rule of law, because the temptation to abuse the enormous power of the government is very real. And that's why we have checks and balances. They're at the fulcrum of our democracy. You agree with that.

ATTY GEN. GONZALES: I agree with that, Senator.

SEN. SCHUMER: I have to say, by the way, that's why I'm disappointed that Chairman Specter wouldn't let us show the clip of the president's speech. Senator Specter said that the transcript speaks for itself. But seeing the speech with its nuances is actually very different from reading the record. And when you watch the speech, it seems clear that the president isn't simply talking about roving wiretaps. He's talking about all wiretaps, because the fact that you don't wiretap citizens without a warrant has been a bedrock of American principles for decades.

Nonetheless, having said that, I am gratified that these hearings have been a lot less partisan than the previous ones we held in this room. And many Republican colleagues have voiced concerns about the administration policy. I want to salute my Republican colleagues for questioning some of these policies -- Chairman Specter and Senator DeWine, Senator Brownback, Senator Graham and others.

But it's not just Republican senators who seriously question the NSA program, but very high-ranking officials within the administration itself. Now, you've already acknowledged that there were lawyers in the administration who expressed reservations about the NSA program. There was dissent. Is that right?

ATTY GEN. GONZALES: Of course, Senator. As I indicated, this program implicates very difficult issues. The war on terror has generated several issues that are very, very complicated.

SEN. SCHUMER: Understood.

ATTY GEN. GONZALES: Lawyers disagree.

SEN. SCHUMER: I concede all those points. Let me ask you about some specific reports. It's been reported by multiple news outlets that the former number two man in the Justice Department, the premier terrorism prosecutor, Jim Comey, expressed grave reservations about the NSA program, and at least once refused to give it his blessing. Is that true?

ATTY GEN. GONZALES: Senator, here's a response that I feel that I can give with respect to recent speculation or stories about disagreements. There has not been any serious disagreement, including -- and I think this is accurate -- there's not been any serious disagreement about the program that the president has confirmed.

There have been disagreements about other matters regarding operations, which I cannot get into. I will also say --

SEN. SCHUMER: But there was some -- I'm sorry to cut you off. But there was some dissent within the administration, and Jim Comey did express at some point -- that's all I asked you -- some reservation.

ATTY GEN. GONZALES: The point I want to make is that, to my knowledge, none of the reservations dealt with the program that we're talking about today. They dealt with operational capabilities that we're not talking about today.

SEN. SCHUMER: I want to ask you again about -- I'm just -- we have limited time.

ATTY GEN. GONZALES: Yes, sir.

SEN. SCHUMER: It's also been reported that the head of the Office of Legal Counsel, Jack Goldsmith, a respected lawyer and professor at Harvard Law School, expressed reservations about the program. Is that true?

ATTY GEN. GONZALES: Senator, rather than going individual by individual --

SEN. SCHUMER: No, I think we're -- this is --

ATTY GEN. GONZALES: -- let me just say that I think differing views that have been the subject of some of these stories does not -- did not deal with the program that I'm here testifying about today.

SEN. SCHUMER: But you are telling us that none of these people expressed any reservations about the ultimate program. Is that right?

ATTY GEN. GONZALES: Senator, I want to be very careful here, because, of course, I'm here only testifying about what the president has confirmed. And with respect to what the president has confirmed, I believe -- I do not believe that these DOJ officials that you're identifying had concerns about this program.

SEN. SCHUMER: Did you -- there are other reports -- I'm sorry; you're not giving me a yes or no answer here. I understand that. Newsweek reported that several Department of Justice lawyers were so concerned about the legal basis for the NSA program that they went so far as to line up private lawyers. Do you know if that's true?

ATTY GEN. GONZALES: I do not know if that's true.

SEN. SCHUMER: Now, let me just ask you a question here. You mentioned earlier that you had no problem with Attorney General Ashcroft, someone else -- I didn't want to ask you about him; he's your predecessor -- people have said had doubts. But you said that you had no problem with him coming before this committee and testifying when Senator Specter asked. Is that right?

ATTY GEN. GONZALES: Senator, who the chairman chooses to call as a witness is up to the chairman.

SEN. SCHUMER: The administration doesn't object to that. Correct?

ATTY GEN. GONZALES: Obviously the administration, by saying that we would have no objection, doesn't mean that we would waive any privileges that might exist.

SEN. SCHUMER: I understand. I got that. But I assume they're the same -- the same would go for Mr. Comey, Mr. Goldsmith, and any other individuals. Assuming you didn't waive executive privilege, you wouldn't have an objection to them coming before this committee.

ATTY GEN. GONZALES: Attorney-client privilege, deliberative privilege, to the extent that there are privileges, it is up to the chairman to decide who he wants to call as a witness. But let me just say that if we're engaged in a debate about what the law is and the position of the administration, that is my job and that's what I'm doing here today.

SEN. SCHUMER: I understand. And you are doing your job. And that's why I am requesting, as I have in the past, but renewing it here today, reaffirmed even more strongly by your testimony and everything else, that we invite these people, that we invite former Attorney General Ashcroft, Deputy Attorney General Comey, OLC Chair Goldsmith, to this hearing and actually compel them to come if they won't on their own. And as for privilege --

SEN. SPECTER: If I might interrupt you for just one moment --

SEN. SCHUMER: Please.

SEN. SPECTER: You'll have extra time.

SEN. SCHUMER: Yes, thank you.

SEN. SPECTER: I think the record was in great shape where I left it. If you bring in Attorney General Ashcroft, that's a critical step.

SEN. SCHUMER: Right.

SEN. SPECTER: It wasn't that I hadn't thought of Mr. Comey, Mr. Goldsmith and other people. But I sought to leave the record with the agreement of the attorney general to bring in former Attorney General Ashcroft.

SEN. SCHUMER: Well, Mr. Chairman, I respect that. I think others are important as well. But I want to get to the issue of privilege here.

SEN. SPECTER: I'm not saying they aren't important. I'm just saying, what's the best way to get them here?

SEN. SCHUMER: Okay. Well, whatever way we can, I'd be all for.

On privilege -- because that's going to be the issue, even if they come here, as I'm sure you will acknowledge, Mr. Chairman -- I take it you'd have no problem with them talking about their general views on the legality of this program, just as you are talking about those -- not to go into the specific details of what happened back then, but their general views on the legality of these programs. Do you have any problem with that?

ATTY GEN. GONZALES: The general views of the program that the president has confirmed. Senator, that's -- again, if we're talking about the general views of --

SEN. SCHUMER: I just want them to be able to testify as freely as you've testified here, because it wouldn't be fair, if you're an advocate of administration policies, you have one set of rules, and if you're an opponent or possible opponent of administration policies, you have another set of rules. That's not unfair, is it?

ATTY GEN. GONZALES: Sir, it's up to the chairman to --

SEN. SCHUMER: No, but would you or the administration -- you as the chief legal officer -- have any problem with them testifying in the same way you did about general legal views of the program?

ATTY GEN. GONZALES: I would defer to the chairman --

SEN. SCHUMER: I'm not asking you, sir -- in all due respect, I'm not asking you what the chairman thinks. He's doing a good job here, and I don't begrudge that one bit.

ATTY GEN. GONZALES: Sir, my answer is I defer to the chairman.

SEN. SCHUMER: I'm asking you what the administration would think in terms of exercising any claim of privilege. You're not going to have -- I'm sorry here -- you're not going to have different rules for yourself, an administration advocate, than for these people, who might be administration dissenters in one way or another, are you?

ATTY GEN. GONZALES: Sir, I don't know if you're asking what are they going to say.

SEN. SCHUMER: I'm not asking you that. Would the rules be the same? I think you can answer that yes or no.

ATTY GEN. GONZALES: If they came to testify?

SEN. SCHUMER: Correct.

ATTY GEN. GONZALES: Well, sir, the client here is the president of the United States. I'm not sure it's in my place to offer --

SEN. SCHUMER: Or his chief --

ATTY GEN. GONZALES: -- offer up a position or my recommendation to you about what I might recommend to

the president of the United States. It would not be appropriate here.

SEN. SCHUMER: But what would be -- I just am asking you, as a very fine, well-educated lawyer, should or could the rules be any different for what you are allowed to say, with privilege hovering over your head, and what they are allowed to say with those same privileges hovering over their heads? Should the rules be any different? If you can't say yes to that, you know, then that's fundamentally unfair. It's saying that these hearings -- it's saying, really, that the administration doesn't have the confidence to get out the whole truth.

ATTY GEN. GONZALES: Sir, my hesitation is, quite frankly, I haven't thought recently about the issue about former employees coming to testify about their legal analysis or their legal recommendations to their client. And that is the source of my hesitation.

SEN. SCHUMER: Okay, I was just -- my time --

SEN. SPECTER: Senator Schumer, take two more minutes from my interruption --

SEN. SCHUMER: Well, thank you, Mr. Chairman.

SEN. SPECTER: -- providing you move to another subject. (Laughter.)

SEN. SCHUMER: Well, okay. I just -- again, I think this is very important, Mr. Chairman.

SEN. SPECTER: Oh, I do too.

SEN. SCHUMER: And I think you would agree. Okay.

SEN. SPECTER: If this were a courtroom, I'd move to strike all your questions and his answers, because the record was so much better off before. (Laughter.)

SEN. SCHUMER: Yeah. Well, I don't buy that, Mr. Chairman.

SEN. SPECTER: But take two more minutes on the condition stated.

SEN. SCHUMER: I don't buy that. I think we have to try to tie down as much as we can here, okay?

Let me go to another bit of questions here. You said, Mr. Attorney General, that the AUMF allowed the president -- that's one of the legal justifications, the Constitution -- to go ahead with this program. Now, under your legal theory, could the government, without ever going to a judge or getting a warrant, search an American's home or office?

ATTY GEN. GONZALES: Well, of course, Senator, any authorization or activity by the president would be subject to the Fourth Amendment. And what you're talking about -- I presume you're talking about a law enforcement effort. This is not a law enforcement --

SEN. SCHUMER: Let me interrupt for a minute. Aren't wiretaps subject to the Fourth Amendment as well?

ATTY GEN. GONZALES: Of course. Of course they are.

SEN. SCHUMER: Okay. So they're both subject. What would prevent the president's theory, your theory, from, given the danger, given maybe some of the difficulties, from going this far?

ATTY GEN. GONZALES: Well, sir, it's hard to answer a hypothetical question in the way that you pose it in terms of how far do the president's authorities extend. However far they may extend, Senator, they clearly extend so far as to allow the president of the United States to engage in electronic surveillance of the enemy during a time of war.

SEN. SCHUMER: Could he engage in electronic surveillance when the phone calls both originated and ended in the United States, if there were al Qaeda suspects?

ATTY GEN. GONZALES: I think that question was asked earlier. I've said that I don't believe that we've done the analysis on that.

SEN. SCHUMER: I didn't ask that. I asked, what do you think the theory is?

ATTY GEN. GONZALES: That's a different situation, Senator. And, again, these kind of constitutional questions -- I could offer up a guess, but these are hard questions.

SEN. SCHUMER: Has this come up? Has it happened?

ATTY GEN. GONZALES: Sir, what the president has authorized is only international phone calls.

SEN. SCHUMER: I understand. Has there been a situation brought to your attention where there were al Qaeda called -- someone suspected of being part of al Qaeda or another terrorist group calling someone from the United States, to the United States?

ATTY GEN. GONZALES: Sir, now you're getting into sort of operations, and I'm not going to respond to that.

SEN. SCHUMER: I'm not asking any specific. I'm asking ever.

ATTY GEN. GONZALES: You're asking about how this program has operated. And I'm not going to answer that question, sir.

SEN. SCHUMER: Thank you, Mr. Chairman.

SEN. SPECTER: Thank you, Senator Schumer. Senator Cornyn.

SEN. JOHN CORNYN (R-TX): Thank you, Mr. Chairman. I think your comments, Mr. Chairman, about this not being a court of law are apt, because I don't think we're going to get resolution about the disagreement among lawyers as to what the legal answer is. But I do believe it's important to have the hearing and to air the various points of view.

But I would hope, and I trust is along the lines of what Senator Schumer stated, is that there would be consensus on the committee and throughout the Congress that we should use all legal means available to us to gather actual intelligence that has the potential of saving American lives. You certainly would agree with that, wouldn't you, General Gonzales?

ATTY GEN. GONZALES: Yes, Senator.

SEN. CORNYN: And some have stated the question like this. They've said, "Well, has the Foreign Intelligence Surveillance Act," which was passed in 1978, "authorized the president to conduct this particular program?"

I have a couple of problems with that question stated that way. Number one, the technology has surpassed what it was in 1978, so our capacity to gain actual intelligence has certainly changed. And the very premise of the question suggests that the president can only exercise the authority that Congress confers.

And when people talk about the law, the law that pertains to this particular question is not just the Foreign Intelligence Surveillance Act, but it includes the Constitution and the authorization for use of military force. Would you agree with that, General Gonzales?

ATTY GEN. GONZALES: Senator, you raise a very important point. People focus on the Foreign Intelligence

Surveillance Act and say, "This is what the words say, and that's the end of it. If you're not following it in total, you're obviously in violation of the law."

That is only the beginning of the analysis. You have to look and see what Congress has done subsequent to that. And then, of course, you have to look at the Constitution. There have been many statements today about "No one is above the law." And I would simply remind -- and I know this doesn't need to be stated -- but no one is above the Constitution either, not even the Congress.

SEN. CORNYN: And clearly the Supreme Court, in the Hamdi case, said what we all know to be the fact, and that is, no president is above the law; no person in this country, regardless of how exalted their position may be or how relatively modest their position may be, we're all governed by the Constitution and laws of the United States.

ATTY GEN. GONZALES: During my confirmation hearings, I talked about Justice O'Connor's statement from Hamdi, that a state of war is not a blank check for the president of the United States. And I said in my hearing that I agreed with that.

SEN. CORNYN: General Gonzales, I regret to say that when I was, just a few minutes ago, watching the crawler or the caption in a cable news network, it referred to domestic surveillance, which strikes me as a fundamental error in the accuracy of the reporting of what's going on here. You've made clear that what's been authorized here is not domestic surveillance; that is, starting from and ending in the United States. This is an international surveillance with known al Qaeda operatives. Correct?

ATTY GEN. GONZALES: I think people who call this a domestic surveillance program are doing a disservice to the American people. It would be like flying from Texas to Poland and saying that's a domestic flight. We know that's not true. That would be an international flight. And what we're talking about are international communications. And so I agree with your point, Senator.

SEN. CORNYN: With regard to the authorization of the use of military force, some have questioned whether it was actually discussed in Congress whether surveillance of international phone calls between al Qaeda overseas and here, whether that was actually in the minds of individual members of Congress when they voted to support the authorization of the use of military force.

It strikes me as odd to say that Congress authorized the commander-in-chief to capture, to detain, to kill, if necessary, al Qaeda, but we can't listen to their phone calls and we can't gather intelligence to find out what they're doing so we can prevent future attacks against the American people.

Now, you've explained your legal analysis with regard to the Hamdi decision and explaining that intelligence is a fundamental incident of war. And I think that makes good sense. And here again, I realize we have some very fine lawyers on the committee and there are a lot of lawyers around the country who've opined on this, some who have been negative, some who have been positive.

I was struck by the fact that John Schmidt, who was associate attorney general during the Clinton Justice Department, wrote what I thought was an eloquent op-ed piece for the Chicago Tribune dated December the 21st, 2005, agreeing with the administration's point of view. That's only to point out that lawyers, regardless of their party affiliation, will have perhaps differing views.

But again, I would hope that what we're not engaged in is either a partisan debate or even an ideological debate, but a legal

But again, I would hope that what we're not engaged in is either a partisan debate or even an ideological debate, but a legal debate on what the constitutional laws of the United States provide for.

Let me turn to another subject that's caused me a lot of concern and that is our espionage laws and the laws that criminalize the intentional leaking of classified information. It's my understanding from the news reports that the Department of Justice has undertaken an investigation to see whether those who actually leaked this program to the New York Times or any other media outlet, might have violated our espionage laws. Is that correct?

ATTY GEN. GONZALES: I can confirm, Senator, that an investigation has been initiated.

SEN. CORNYN: Does that investigation also include any potential violation for publishing that information?

ATTY GEN. GONZALES: Senator, I'm not going to get into specific laws that are being looked at, but obviously, our prosecutors are going to look to see all the laws that have been violated and if the evidence is there, they're going to prosecute those violations.

SEN. CORNYN: Well, you may give me the same answer to this next question, but I'm wondering, is there any exclusion or immunity for the New York Times or any other person to receive information from a lawbreaker seeking to divulge classified information? Is there any explicit protection in the law that says that if you receive that and you publish it, you are somehow immune from a criminal investigation?

ATTY GEN. GONZALES: Senator, I'm sure the New York Times has their own great set of lawyers and I would hate in this public forum to provide them my views as to what would be a legitimate defense.

SEN. CORNYN: Well, it's -- there's a lot of very strange circumstances surrounding this initial report in the New York Times, including the fact that the New York Times apparently sat on the story for a year and then, of course, the coincidence -- some might say -- that the story was broken on the date that Congress was going to vote -- the Senate was going to vote on reauthorization of the Patriot Act. But we'll leave that, perhaps, for another day.

SEN. CORNYN: I believe I will yield the rest of my time back. Thank you, Mr. Chairman.

SEN. SPECTER: Thank you very much, Senator Cornyn.

SEN. RICHARD DURBIN (D-IL): Thank you very much, Mr. Chairman. Thank you, Attorney General, for being here.

During the course of this hearing, you have referred to FISA several times as a useful tool -- a useful tool in wiretapping and surveillance. And I've thought about that phrase, because it's a phrase that's been used by the White House, too. Referring to FISA as a useful tool in wiretapping is like referring to speed limits and troopers with radar guns as useful tools on a motoring trip.

I think FISA is not there as a useful tool to the administration. It is there as a limitation on the power of a president when it comes to wiretapping. And I think your use of that phrase, useful tool, captures the attitude of this administration toward this law -- we'll use it when it doesn't cause a problem. We'll ignore it when we have to and I think that's why we're here today.

And I'm just -- I'm curious, Mr. Attorney General, as we get into this and I look back on some of your previous testimony and what you said to this committee in confirmation hearings and the like, how far will this administration go under the theories which you stated today to ignore or circumvent laws like FISA? I asked you during the course of the last -- your confirmation hearing -- the question of this whole power of the commander in chief. I wish I could play it to you here, but there's a decision made by the committee that we aren't going to allow that sort of thing to take place. But I do believe that if I could play, you would be asked to explain your answer to a question, which I posed to you.

And the question was this -- Mr. Attorney General, has this president ever invoked that authority as commander in chief or otherwise to conclude that a law was unconstitutional and refused to comply with it? Mr. Gonzales -- I believe

that I stated in my June briefing about these memos that the president has not exercised that authority.

You said to us today, several times, that the president is claiming his power for this domestic spying -- whatever you want to call it -- terrorist surveillance program -- because of the president's inherent powers, his core constitutional authority of the executive branch. And so I have to ask you point blank, as Senator Feingold asked you earlier, you knew when you answered my question that this administration had decided that it was going to basically find away around the FISA law based on the president's -- as you called it -- inherent constitutional powers.

So how can your response be valid today in light of what we now know?

ATTY GEN. GONZALES: Oh, it's absolutely valid, Senator. The -- and this is going to sound repetitious -- but it has never been our position that we are circumventing or ignoring FISA -- quite the contrary. The president has authorized activities that are totally consistent with FISA, with what FISA contemplates.

I have indicated that I believe that putting aside the question of the authorization to use military force, that while it's a tough legal question as to whether or not Congress has the authority under the Constitution to cabin or to limit the president's constitutional authority to engage in an electronic surveillance of the enemy. that is not -- that is not a question that we even need to get to. It has always been our position that FISA can be and must be read in a way that it doesn't infringe upon the president's constitutional authority.

SEN. DURBIN: So let me read to you what your own Justice Department just issued within the last few weeks -- in relation to the president's authority, the NSA program and FISA. Because the president -- I quote -- "Because the president also has determined that NSA activities are necessary in the defense of the United States from a subsequent terrorist attack and armed conflict with al Qaeda," I quote, "FISA would impermissible interfere with the president's most solemn constitutional obligation -- to defend the United States against foreign attack." You can have it both ways.

ATTY GEN. GONZALES: And that's why --

SEN. DURBIN: You can't tell me that you're not circumventing it and then publish this and say that FISA interferes with the president's constitutional authority.

ATTY GEN. GONZALES: And that's why you have to interpret FISA in a way where you don't T-up that very difficult constitutional question.

SEN. DURBIN: What you can't do --

ATTY GEN. GONZALES: -- constitutional (avoidance ?).

SEN. DURBIN: What you have to do is take out the express language in FISA which says it is the exclusive means -- it is exclusive. And the way you take it out is by referring to -- and I think you've said it over and over again -- you just have to look at that phrase, you say, except as otherwise authorized by statute.

Senator Feinstein and I were struggling. We're looking through FISA -- where is that phrase, except as otherwise authorized by statute? It's not in FISA. It's not in the FISA law. You may find it in the criminal statute and may want to adopt it by reference, but this FISA law signed by a president and the law of the land is the exclusive way that a president can wiretap.

And I want to ask you, if this is exclusive, why didn't you take advantage of the fact that you had and the president had such a strong bipartisan support for fighting terrorism that we gave the president the Patriot Act with only one dissenting vote? We've supported this president with every dollar he's asked for to fight terrorism. Why didn't you come to this Congress and say, there are certain things we need to change, which you characterize as cumbersome and burdensome in FISA. Why didn't you work with us to make the law better and strong and more effective when you

knew that you had a bipartisan consensus behind you?

ATTY GEN. GONZALES: Senator, the primary criminal code -- criminal provision in FISA, Section 109, 50 USC 180 -- it is page 179 in one of these books -- provides that a person is guilty of an offense if he intentionally engages in electronic surveillance under cover of law accept as authorized by statute.

This provision means that you have to engage in electronic surveillance as provided here, accept as otherwise provided by statute. And this is the provision that we're relying upon. It's in the Foreign Intelligence Surveillance Act.

SEN. DURBIN: It's Title 18. But let me just tell you, what you don't want to read to us --

ATTY GEN. GONZALES: Sir, it's not Title 18.

SEN. DURBIN: A Foreign Intelligence Surveillance Act of 1978 shall be the exclusive means by which electronic surveillance -- as defined in Section 101 as to check, interception of domestic wire electronic communication may be conducted.

And so what you said is, well, when you authorized the war you must have known that we were going to really expand beyond FISA. I've got the book here. You can look through it if you like. There's not a single reference in our passing -- that AUMF that we talk about -- Authorized Use of Military Force -- not a single reference to surveillance and intelligence in the manner in which you described it.

ATTY GEN. GONZALES: Sir, there's probably not a single reference to detainment of American citizens, but the Supreme Court has said that that is exactly what you've authorized because it is a fundamental incident of waging war.

SEN. DURBIN: So since you've quoted that repeatedly, let me read what that court has said, we conclude -- Hamdi Decision -- we conclude the detention of individuals falling into the limited category we are considering for the duration of the particular conflict in which they are captured is so fundamental and accepted an incident to war to be an exercise of necessary and appropriate force.

ATTY GEN. GONZALES: No question. That case was not about electronic surveillance. I will concede that.

SEN. DURBIN: But I'll tell you something else, Mr. Attorney General, if you would then read, I think, the fine reasoning of Justice O'Connor, she comes to a point which brings us here today -- and I thank the chairman for allowing us to be here today -- and this is what she says in the course of this decision: It is during our most challenging and uncertain moments that our nation's commitment to due process is most severely tested. And it is in those times that we must preserve our commitment at home to the principles for which we fight abroad.

We have said repeatedly as nominees for the Supreme Court have come here, do you accept the basis of Hamdi? That a war is not a blank check for a president? They have said, yes, that's consistent with Jackson and Youngstown. Now what we hear from you is that you are going to take this decision in Hamdi, and build it into a way to avoid the most basic statute when it comes to electronic surveillance in America. A statute which describes itself as the exclusive means by which this government can legally do this.

ATTY GEN. GONZALES: Senator, I think that in reading that provision you just decided to -- you have to consider Section 109. Section 109 contemplates an additional authorization by the Congress. Congress provided that additional authorization when it authorized the use of military force following the attacks of 9/11.

SEN. DURBIN: Well, the last thing I'd like to say -- and I only have a minute to go -- is the greatest fear that we have is that what this president is now claiming is going to go far beyond what you've described today. What you've described today is something we would all join in on a bipartisan basis to support -- use every wiretap capacity you have to stop dangerous terrorists from hurting Americans.

If you came to Capitol Hill and asked us to change a law in a reasonable way to reach that goal, you'd have the same bipartisan support. Our concern is what this president is asking for will allow this administration to comb through thousands of ordinary Americans e- mails and phone calls. In the audience today is Richard Fleischer (sp) of Willowbrook, Illinois. I don't know if Mr. Fleischer (sp) is still here. Mr. Fleischer (sp) wrote to the NSA and asked if he had been wiretapped because he had has conversations with people overseas. And after several letter that he sent back and forth, the best he could get from the National Security Administration is that they would neither confirm nor deny the existence of records responsive to his request.

Ordinary Americans wondering of their telephone calls, if their e-mails overseas have been wiretapped and there is no safeguard for their liberty and freedom. What we have today is your announcement that career professionals and experts will watch out for the freedoms of America. Career professionals and experts, sadly, in our nation's history have done things in the past that we're not proud of. Career professionals have made bad decisions -- Japanese internment camps, enemies list. What we really rely on is the rule of law and the Constitution -- safeguards we can trust by people we can see. And when it comes to some person working at NSA, I don't think it gives us much comfort.

SEN. SPECTER: Thank you, Senator Durbin.

Before yielding to Senator Brownback, I want to announce that I'm going to excuse myself for just a few minutes. We're starting on floor debate this afternoon at 3:00 on the Asbestos Reform Bill on which Senator Leahy and I are cosponsors, and I am scheduled to start the debate at 3:00 and I will return as soon as I have made a floor statement. And in the interim, Senator Hatch has agreed to chair the hearing.

Senator Brownback, you're recognized.

SEN. SAM BROWNBACK (R-KS): Thank you, Mr. Chairman. I appreciate the hearing. Attorney General, thank you for being here.

I want to look at the reason we're in this war on terrorism. I want to talk about the length of time we may be in the war on terrorism and then I want to look at FISA's use forward from this point in the war on terrorism.

I don't need to remind the attorney general -- but I certainly would my colleagues -- that we are very actively engaged in a war on terrorism today. January 19th of this year, Osama bin Laden in a tape says this, quote, "The reason why we didn't have such an operation will take place and you will see such operations, by the grace of God." And by that he's talking about more 9/11's and that was January 19th, 2006.

Al-Zawahiri -- number two person -- January 30th of this year says this, Bush, do you know where I am? Among the Muslim masses enjoying their care with God's blessings and sharing with them their holy war against you until we defeat you, God willing. The lion of Islam, Sheik Osama bin Laden, may God protect him, offered you a decent exit from your dilemma, but your leaders who are keen to accumulate wealth insist on throwing you in battles and killing your souls in Iraq and Afghanistan and, God willing, on your own land.

I just want to remind people that as we get away from 9/11 and 2001, we not forget that we're still very much in a war on terrorism and people are very much at war against us.

And we're talking about probably one of the lead techniques we can use in this war, which I would note recent testimony of General Hayden said this about the technique of the information you're using right now. He said, quote, "Had this program been in effect prior to 9/11, it's my professional judgment that we would have detected some of the 9/11 al Qaeda operatives in the United States and we would have identified them as such."

Mr. Attorney General, I don't know if you have a different opinion from General Hayden on that, but --

ATTY GEN. GONZALES: I never have a different opinion from General Hayden on the intel capabilities that

we're talking about here. Both he and Director Muller have recently testified about the importance of the terrorist surveillance program. Now General Hayden did say it's been very successful, that we've gotten information we would not have otherwise gotten, that it has helped us, I think he said, deter and detect attacks here and abroad. FBI Director Muller said it was a valuable tool, had helped identify would-be terrorists in the United States, and helped identified individuals providing material support to terrorists. So those are the experts saying how valuable this tool has been.

SEN. BROWNBACK: Having said that, we're -- and I've read through most of your white paper material and I've looked at a great deal of it. I'm -- I'm struck and I'm -- I'm -- I think we have an issue we need to deal with. Part of what we're working off of is a war declaration dated September 18th, 2001 and a war declaration on Afghanistan, and a war declaration October 16th, 2002 on the use of military force in Iraq. And all necessary force and all necessary -- "the president is authorized to use all necessary and appropriate force against those nations, organizations or persons he determines planned, authorized, committed or aided the terrorist attacks."

It strikes me that we're going to be in this war on terrorism possibly for decades. Maybe not, but this could be the Cold War of our generation. Maybe it doesn't go that period of time, but it has the possibilities of going for some extended period of time. And I share Senator DeWine's concern that we should look then at the FISA law and make sure that as we move forward in this, that we're not just depending upon these authorizations of war to say that that puts us in a superior position under the Article II powers, but that to maintain the support of the American public, to have another set of eyes also looking at this surveillance technique is an important thing in maintaining the public's support for this.

And so I want to look and direct you to looking at the FISA law in particular. And you've made some comments here this morning, I think have been -- today that have been very well -- very well stated and thought through. You've talked at one point not well -- the FISA law was not well structured to the needs of today's terrorist war effort. That law was passed, what, 27 years ago or something of that nature, and certainly didn't contemplate a war on terrorism like we're in today. And I want to look specifically at how we could amend that FISA law, looking at a possible decades-long war on terrorism.

Now one of the areas you've talked about that's cumbersome is the 72-hour provision within the law, if I'm -- if I'm gathering what you're saying correctly. Congress extended this period from 24 to 72 hours in 2001. Just looking narrowly at what would need to be done to use the FISA authority more broadly and still be able to stop terrorists, if that is extended further, would it make it more likely that you would use the FISA process if that's extended beyond 72 hours?

ATTY GEN. GONZALES: It's hard to say, Senator because it's -- you know, whether it's 24, 72, whatever, I have got to make a determination under the law that at the time I grant emergency authorization that all the requirements of FISA are met. I think General Hayden said it best yesterday: this is not a 72-hour sort of hall pass. I've got to know when I grant that authorization whether I then have 24 or 72 hours to submit a written application to the court. I've got to know at the time I say yes, go forward, that all the requirements of FISA are met. That's -- that's the problem.

If I could just also make one final point --

SEN. BROWNBACK: Fair enough.

ATTY GEN. GONZALES: -- there was not a war declaration, either in connection with -- with al Qaeda or in Iraq. It was an authorization to use military force. I only want to clarify that because there are implications. Obviously, when you talk about a war declaration, you're possibly talking about effecting treaties, diplomatic relations. And so there is -- there is a distinction in law and in practice, and we're not talking about a war declaration. This is an authorization only to use military force.

SEN. BROWNBACK: Looking forward in the war on terrorism and the use of FISA and this committee's desire I believe to have the administration whereever possible and more frequently use FISA -- and you've noted you've used it

more this past year than the year before -- what specific areas would make this decision on your part easier, more likely to use the FISA process?

ATTY GEN. GONZALES: Well, Senator, if you're talking about domestic surveillance in a peacetime situation, for other kinds of terrorists beyond al Qaeda --

SEN. BROWNBACK: No, I'm talking about --

ATTY GEN. GONZALES: -- I'm not sure --

SEN. BROWNBACK: -- the war on terrorism.

ATTY GEN. GONZALES: Sir, I would like the opportunity to think about that and maybe talk to the experts in the department. I think it would have a better sense about what kind of specific things -- I can say that -- that the Patriot Act includes a provision which allows these orders to stay a long -- stay in place a longer period of time before they're renewed. It is quite burdensome. The fact that these things expire, we then have to go back and get it renewed, I just -- that just places an additional burden on our staff. But I would like to have the opportunity to get back to you about what other kinds of specific changes might be helpful.

SEN. BROWNBACK: Well if -- if you could because I think we're going to be in this for a period of time and we're going to be in it for succeeding administrations in this war on terrorism. And probably our most valuable tool that we have is information, early information, to be able to cut this off. So the American public I think clearly wants us to be able to get as much information as we can, and yet I think we need to provide a process that has as much security to the American public that there's no abuse in this -- in this system. This is about us trying to protect people and protect people in the United States.

And I want to know, too, presidential authority that you're protecting -- this has been talked about by Clinton administration attorney general before, many others; it's not just this administration at all, as others have specifically quoted. But I do think as this wears on, we really need to have -- have those thoughts at how we can make the FISA system work better.

ATTY GEN. GONZALES: Senator, we are as likewise concerned about ensuring that we protect the rights of all Americans.

SEN. BROWNBACK: And I'm sure you are, and I -- and I appreciate that. I want you to protect us from security attacks, too. And bin Laden has -- to my knowledge, when he normally makes a threat, he has followed through on these. This is a very active and live area. So I want to see if we can make that law change where it can work for a long-term war on terrorism.

Thank you, Mr. Chairman.

SEN. SPECTRE: Senator Leahy?

SEN. PATRICK LEAHY (D-VT): Thank you, Mr. Chairman.

You know, incidentally, Senator Brownback rightfully pointed out the date when FISA was enacted. But of course, we have updated it five times since 9/11, two of those when I was chairman. The year 2000, the last year of the Clinton administration, they used the FISA court one hundred and -- I mean, 1,005 times. The year of 1911 -- I mean, September 11 -- your administration there actually used it less times even than the Clinton administration used it before.

I'm just curious. You know, I started this morning -- I asked you a very straightforward question. I told you I'd come back to it, so I'm sure you've had time to check for the answer during the lunch hour. So I come to you again with it. When did the Bush administration come to the conclusion that the congressional resolution authorizing the use of

military force against al Qaeda also authorized warrant-less wire tapping of Americans inside the United States?

ATTY GEN. GONZALES: Sir, the, the authorization of this program began --

SEN. LEAHY: Can't hear you. Could you pull your mic a little bit closer?

ATTY GEN. GONZALES: Pardon me. The authorization regarding the terrorist surveillance program occurred subsequent to the authorization to use military force and prior to the Patriot Act.

SEN. LEAHY: Okay. So what you call "terrorist surveillance" I'm going to call the breaking of the Foreign Intelligence Security -- I'm asking, when -- when did you decide -- when did you decide that the authorization for use of military force gave you the power to do this? I mean, you were -- you were White House counsel then. What date did it give you the power?

ATTY GEN. GONZALES: Well, sir, I can't give you specific dates about when --

SEN. LEAHY: That's what I asked you this morning, and you had the time to go and look. I mean, you -- you had to sign that or sign off on that before the president -- when did you have -- when did you reach the conclusion --

ATTY GEN. GONZALES: Sir, I -- I --

SEN. LEAHY: -- that you didn't have to follow FISA?

ATTY GEN. GONZALES: Sir, I'm not going to give an exact date as to when that -- the program actually commenced.

SEN. LEAHY: Why not?

ATTY GEN. GONZALES: But it has always been -- it's always been the case -- because that's an operational detail, sir. I've already indicated the chairman has invited me -- the committee has invited me here today to talk about the legal analysis of what the president authorized.

SEN. LEAHY: We're asking for the legal analysis. I mean, obviously you had to -- you had to make a determination that you had right to do this. When did you make -- when did you make the determination --

ATTY GEN. GONZALES: From the very --

SEN. LEAHY: -- that the AUMF gave you the right to do this?

ATTY GEN. GONZALES: From the very outset, before the program actually commenced, it has always been the position that -- that FISA cannot be interpreted in a way that infringes upon the present constitutional authority -- that FISA must be interpreted, can be interpreted in a way that --

SEN. LEAHY: Did you tell anybody that when you were up here seeking the Patriot Act and seeking the changes in FISA? Did you tell anybody you had already determined -- it was your testimony here today that you made the determination virtually immediately that you had this power without using FISA.

ATTY GEN. GONZALES: Well, sir, the fact -- the fact that -- that we were having discussions about the Patriot Act and there wasn't a specific mention about electronic surveillance with respect to this program -- I would remind the committee that there was also discussion about detention in connection with the Patriot Act discussions. Justice Souter in the Hamdi decision made that as an argument, that clearly Congress did not authorize --

SEN. LEAHY: (Judge ?) Gonzales, I'm not asking about what happens when you catch somebody on a battlefield

and detain them. I'm not asking about what you do in the battlefield in our failed attempt to catch Osama bin Laden, which is what we were actually asking the administration to do. I'm not asking about what happens in that battlefield. I'm asking, why did you feel that this -- now your testimony is that virtually immediately you determined you had the power to do this warrant-less wire tapping because of AUMF. You didn't ask anybody up here. Did you tell anybody that you needed something more than FISA?

ATTY GEN. GONZALES: Sir I don't, I don't recall -- did I tell anyone in Congress or tell --

SEN. LEAHY: Congress. Let's take Congress first.

ATTY GEN. GONZALES: Sir, I don't recall having conversations with anybody in Congress about it.

SEN. LEAHY: All right. Do you recall anybody on this committee, which actually is the one that would be amending FISA, was told?

ATTY GEN. GONZALES: Sir, I have no personal knowledge that anyone in this committee was told.

SEN. LEAHY: Now apparently, then, according to your interpretation, Congress -- and a lot of Republicans and a lot of Democrats disagree with you on this -- when we voted for authorization for military force, that we're authorizing warrant-less wiretapping. Did we -- were we authorizing you to go into people's medical records here in the United States by your interpretation?

ATTY GEN. GONZALES: Senator, I -- whatever the limits of the president's authority given by -- under the authorization to use military force and his inherent authority as commander in chief in a time of war, it clearly includes electronic surveillance of the enemy.

SEN. LEAHY: Well, just let it note that you did not answer my question. But here you also said we've had discussions with the Congress in the past, certain members of Congress, as to whether or not FISA could be amended to allow us to adequately deal with this kind of threat, were advised them that would be difficult if not impossible. That's your statement. All right. Who told you that?

ATTY GEN. GONZALES: Senator, there was -- there was discussion with a bipartisan group of Congress -- leaders in Congress, leaders of the Intel Committee -- to talk about legislation. And the consensus was that obtaining such legislation, the legislative process is such that it could not be successfully accomplished without compromising the program.

SEN. LEAHY: When did -- when did they -- when did they give you that advice?

ATTY GEN. GONZALES: Sir, that was sometime in 2004.

SEN. LEAHY: Ah. Two years later? I mean, you've been doing this wiretapping for three years and then suddenly you come up here and say, oh, by the way guys, could we have a little bit of authorization for this? Is that what you're saying?

ATTY GEN. GONZALES: Sir, it's always been our position that the president has the authority under the authorization to use military force and --

SEN. LEAHY: It's always been your position --

ATTY GEN. GONZALES: -- under the Constitution.

SEN. LEAHY: -- but, frankly, it flies in the face of the statute, Mr. Attorney General. And I doubt very much, if one single person of Congress would have known that was your position, had you not known the newspapers were

going to print what you were doing -- not that anybody up here knew it. When you found out the newspapers were going to print it, you came up here.

Did you talk to any member of the Judiciary Committee that would actually write it? And let me ask you this: did any member of this committee -- this Judiciary Committee that has to write the law -- did anybody here tell you we couldn't write a law that would allow you to go after al Qaeda in the way you're talking about?

ATTY GEN. GONZALES: Sir, I don't believe there were any discussions with any members of the Judiciary Committee about --

SEN. LEAHY: Oh, even though we're the ones that have to write the law, and you're saying that you were told by members of Congress we couldn't write a law that would fit it, and now you tell us that the committee that has to write the law never was asked?

ATTY GEN. GONZALES: We had discussions --

SEN. LEAHY: Does this sound like a CYA on your part? It does to me.

ATTY GEN. GONZALES: We had discussions with a bipartisan leadership of the Congress about this program.

SEN. LEAHY: But not in front of this committee. We have both Republicans and Democrats on this Committee, you know.

ATTY GEN. GONZALES: Yes sir, I do know that.

SEN. LEAHY: And this committee has give you twice under my -- twice under my chairmanship, we have given you five amendments to FISA because you requested it. But this, you never came to us.

Mr. Attorney General, can you see why I have ever reason to believe we never would have found out about this if the press hadn't? Now it's been talked about, well, let's go prosecute the press.

Heavens, thank God we have a press that at least tells us what the heck you guys are doing, because you're obviously not telling us.

ATTY GEN. GONZALES: Sir, we have advised the bipartisan leadership of the Congress and the intel committees about this program.

SEN. LEAHY: Well, did you tell them that before the passage of the U.S.A. Patriot Act?

ATTY GEN. GONZALES: Senator, I don't recall when the first briefing occurred. But it was shortly -- my recollection is that it was shortly after the program was initiated.

SEN. LEAHY: Okay, well, let me ask you this then. You say several years after it started you came up here and talked to some group of members of Congress. The press reported that the president's program of spying on Americans without warrants was shut down for some time in 2004. That sounds like the time you were up here. So if the president believed the program was necessary and legally justified, why did he cut it -- why did he shut it down?

ATTY GEN. GONZALES: Sir, you're asking me about the operations of the program, and I'm not going to get into that.

SEN. LEAHY: Of course. I'm sorry, Mr. Attorney General. I forgot: you can't answer any questions that might be relevant to this. (Laughter.) Well, if the president has that authority, does he also have the authority to wiretap Americans' domestic calls and e-mails under this -- let me finish -- under this authority, if he feels it involves al Qaeda

activity? I'm talking about within this country. Under this authority you've talked about, does he have the power, under your authority, to wiretap Americans within the United States if they're involved in al Qaeda activity?

ATTY GEN. GONZALES: Sir, I've been asked this question several times --

SEN. LEAHY: I know, and you've had somewhat of a vague answer, so I'm asking again.

ATTY GEN. GONZALES: And I've said that that presents a different legal question, a possibly tough constitutional question, and I'm -- I am not comfortable, just off the cuff, talking about whether or not such -- such activity would in fact be constitutional. I will say that that is not what we're talking about here.

SEN. LEAHY: Are you doing that?

ATTY GEN. GONZALES: That is not what the president has authorized.

SEN. LEAHY: Are you doing that?

ATTY GEN. GONZALES: I can't give you assurances. That is not what the president has authorized through this program.

SEN. LEAHY: Are you doing that? Are you doing that?

ATTY GEN. GONZALES: Senator, you're asking again about operations, what are we doing.

SEN. LEAHY: Thank you.

SEN. HATCH: Throughout this process, you don't know when it began, but at least eight members of Congress have been informed about this -- about what has been disclosed by people who have violated the law in disclosing it, and by the media that has printed the disclosures. Is that correct?

ATTY GEN. GONZALES: That is generally correct, sir. Yes, sir.

SEN. HATCH: Did you have one complaint about the program from any of the eight -- and that was bipartisan, by the way, those eight people.

ATTY GEN. GONZALES: It was a bipartisan briefing.

SEN. HATCH: They were Democrats -- four Democrat leaders in the Congress and four Republican leaders in the Congress; is that right?

ATTY GEN. GONZALES: It was a bipartisan briefing, yes, sir.

SEN. HATCH: Did you have any gripes or complaints about what was disclosed to them, to the best of your recollection?

ATTY GEN. GONZALES: Well, again, I want to be careful about speaking for members, but --

SEN. HATCH: I'm not asking you to state for members. I'm asking if you had any gripes or complaints.

ATTY GEN. GONZALES: I think -- and again, I wasn't present --

SEN. HATCH: Or suggestions --

ATTY GEN. GONZALES: I wasn't present at all the briefings, but for briefings that I was present at, they received

very detailed briefings about these operations. They were given ample opportunity to ask questions, they were given ample opportunity to express concern.

SEN. HATCH: Now, you were somewhat criticized here in some of the questions that -- that your argument that the authorized use of military force is a faulty argument, because the FISA Act does not really talk about -- except as authorized by statute. But you've pointed out that Section 109 or, if you want to be more specific, Section 1809 of Title 50, Chapter 36 of Chapter 1-1809 -- it does say that a person is guilty of an offense if he intentionally engages in electronic surveillance under color of law, except as authorized by statute.

ATTY GEN. GONZALES: And that is the main criminal prohibition in engaging -- against engaging in electronic surveillance, except as otherwise provided for by a statute or except -- I mean, except as otherwise provided by FISA, or except as otherwise provided by a statute.

SEN. HATCH: Now this authorized use of military force enables you, quote, "to use all necessary and appropriate force against the national -- against the nations, organizations and persons the president determines planned, authorized, committed or aided the terrorist attacks." Is that correct?

ATTY GEN. GONZALES: This is a very important point, Senator. Think about it: the authorization doesn't identify the -- it never mentions the word al Qaeda. It authorizes the president to engage in all necessary and appropriate force to identify those HE determines -- who the president determines, and the president is not able to do that without information, without intelligence, without the kind of electronic surveillance we're talking about today.

SEN. HATCH: That's right. As someone who helped to write the Patriot Act, the original Patriot Act, I can't help but express the awareness of those of us around here that here we are, well over a month after the expiration of the Patriot Act, and we keep renewing it from month to month because we can't get Congress to really agree on what the changes should be. Is that a fair assessment?

ATTY GEN. GONZALES: Well, what I will say is I think the tools of the Patriot Act are important, and I hope that they are reauthorized quickly.

SEN. HATCH: But the reason -- the reason I'm bringing that up is because at one time, at least one report was is that one of these eight members was asked, who had the program disclosed to them, or at least remarked, that he didn't think that a statute could be passed to resolve these issues.

ATTY GEN. GONZALES: I don't want to attribute to any particular member that statement. What I will say --

SEN. HATCH: You don't have to do that. But is that true?

ATTY GEN. GONZALES: It was a consensus that pursuing the legislative process would result, likely, in compromising the program.

SEN. HATCH: In other words, it's not easy to get things through 535 members of Congress -- 435 in the House and 100 in the Senate. Now, I know that you love the Congress and will not find any fault with any of us.

ATTY GEN. GONZALES: Sir, you've been at this a little bit longer than I have, but it's only been my experience that it's sometimes difficult.

SEN. HATCH: Yeah, it is.

Is it not true that one check on the president's power to operate the NSA's surveillance program is the Congress's power over the purse, as listed in Article I, Section 8 of the Constitution.

ATTY GEN. GONZALES: Absolutely. I think even those who have served in the pro-executive camp in terms of

the allocation of constitutional powers in a time of war would have to concede that the power of the purse is an extremely strong check on the president, the commander in chief.

SEN. HATCH: Well, I've noticed that while many in Congress have sharply criticized the president and the NSA program that we've been discussing here, I am not aware of any member of Congress introducing legislation to end the program, through either an authorization or an appropriations mechanism. But from what we know about the intent of the program today, I expect a few members of either the House or the Senate would vote to eliminate this program or cut off its funding. And the reason I state that is because all of us are concerned about this battle that we're waging, that this is not an easy battle. This is a war unlike any war we've ever had before, and it's a very secret war on their side. And I think the administration has taken a position that we've got to be very careful about disclosures on our side as well. Is it not true that the disclosures that have occurred have very definitely hurt our ability to gather intelligence?

ATTY GEN. GONZALES: The director of the CIA, I believe, has publicly commented that it has hurt us.

SEN. HATCH: Well, it's important, General, to bring up that President Clinton's administration ordered several warrantless searches on the home and property of a domestic spy, Aldrich Ames. That's true, isn't it?

ATTY GEN. GONZALES: That is correct, sir.

SEN. HATCH: That was a warrantless set of searches.

ATTY GEN. GONZALES: That is correct, sir.

SEN. HATCH: Isn't -- and the Clinton administration also authorized a warrantless search of the Mississippi home of a suspected terrorist financier. Is that correct?

ATTY GEN. GONZALES: I think that is correct, sir.

SEN. HATCH: The Clinton Justice Department authorized these searches because it was the judgment of Deputy Attorney General Jamie Gorelick, somebody I have great admiration for, that -- and let me quote her. It has been quoted before, but I think it's worth quoting it again. This is the deputy attorney general of the United States under the -- in the Clinton administration:

"The president," quote -- she said: "The president has inherent authority to conduct warrantless physical searches for foreign intelligence purposes." Now, this was against the domestic people. "And the rules and methodologies for criminal searches are inconsistent with the collection of foreign intelligence and would unduly frustrate the president in carrying out his foreign intelligence responsibilities."

You're aware of that quote?

ATTY GEN. GONZALES: I am aware of it, yes, sir.

SEN. HATCH: Well, if the president has inherent ability to surveil American citizens in national security cases during peacetime, I guess what's bothering me: How could it be that president Bush is precluded, as some have argued, from surveilling al Qaeda sources by intercepting foreign calls into this country to people who may be al Qaeda or affiliated with al Qaeda or affiliated with somebody who is affiliated with al Qaeda? How can that be?

ATTY GEN. GONZALES: Senator, I think that the president's authority as commander in chief obviously is stronger during a time of war. If the authorization to use military force did not exist or were repealed, or were not interpreted in the way we're advocating, then it seems to me you're teeing up a fairly difficult constitutional question as to whether or not Congress can constitutionally limit the president's ability to engage in electronic surveillance of the enemy during a time of war.

SEN. HATCH: Well, we were aware of the Clinton administration's approaches. I don't know of any Republicans who raised Cain about that. Walter Dellinger, the former head of the Office of Legal Counsel under President Clinton, in a final opinion published on July 14th, 1994, wrote, quote: "Specifically we believe that the prohibition on destruction of aircraft would not apply to the actions of United States military forces acting on behalf of the United States during a state of hostility. We note specifically that the application of the provision to acts of the United States military personnel in a state of hostilities could lead to absurdities. For example, it could mean in some circumstances that military personnel would not be able to engage in reasonable self defense without subjecting themselves to the risk of criminal prosecution."

General, do you believe Walter -- that Walter Dellinger, who is now a critic of the president's authorization of wartime surveillance of al Qaeda, was correct in 1994?

ATTY GEN. GONZALES: Sir, I haven't studied that opinion in a while, but it sounds like it would be correct, in my judgment.

SEN. HATCH: All right.

Let me just bring up again, as I understand it, just so we can repeat it one more time -- the administration takes the position that a firmer statute on top of the Section 109, the FISA Act, would also complement the act, and the authorized use of the military force, granted by Congress, is an acceptable legitimate statute that goes to the point that I made earlier, to use all necessary and appropriate force against the nations, organizations or persons the president determines planned, authorized, committed, or aided the terrorists' attacks, and that that justifies doing what you can to interdict these foreign terrorists who are calling into our country to people who may also be affiliated.

As I understand it, that's part of it. The second part of it is the fact that you are citing that the president does have inherent powers under Article II of the Constitution to -- to engage in these activities. And thirdly, that you have not violated the Fourth Amendment of the Constitution, because the position you're taking under these circumstances, with the obligation to protect this country, are reasonable searches and seizures?

ATTY GEN. GONZALES: I think clearly these searches are reasonable given the circumstances -- the fact that we have been attacked by enemy here within this country. I think it would fall within the special means jurisprudence of the Supreme Court that would allow warrantless searches.

Let me just say that an important component of our arguments relies upon the canon of constitutional avoidance, because there are -- I heard some members of Congress -- some members of the committee say they're not sure they buy the authorization to use military force analysis. If our interpretation is simply, fairly possible -- if it is only fairly possible, and the court has held that that interpretation must be adopted if it means that we can avoid a tough constitutional issue.

SEN. HATCH: Thank you, sir, my time is done.

SEN. SPECTER: Senator Feinstein.

SEN. DIANNE FEINSTEIN (D-CA): Thank you, Mr. Chairman.

Mr. Chairman, I want to respond to you on the Jamie Gorelick- Aldrich Ames situation, because, in fact, the law was changed directly after the Aldrich Ames case. I called -- because I heard you say this before, so I called Jamie Gorelick, and I asked her to put this in writing. She has done so, and I have it before me now.

And she points out in this letter that her '94 testimony arose in context of congressional consideration of an extension of FISA to cover physical searches. And at the time, FISA covered only electronic surveillance such as wiretaps. In 1993 the attorney general had authorized foreign intelligence physical searches in the investigation of

Aldrich Ames, whose counsel thereafter raised legal challenges to those searches. Point: There wasn't a law at that time.

Then she goes on to say that the Clinton administration believed, quote, "It would be better if there were congressional authorization and judicial oversight of such searches. My testimony did not address inherent president authority to conduct electronic surveillance, which was already covered by FISA."

I would ask that this letter, and her testimony, be entered into the record.

SEN. HATCH: Without question, it will be entered into the record.

SEN. FEINSTEIN: Thank you. You know, I respect you greatly, but I think that's a bit of a red herring.

SEN. HATCH: But you need to also quote -- in the same letter she said, "My testimony did not address whether there would be inherent authority to conduct physical searches if FISA were extended to cover physical searches." And she goes on -- but we'll put it into the record.

SEN. SESSIONS: Mr. Chairman, could I just raise one point? Just one point?

SEN. FEINSTEIN: If I have extra time.

SEN. HATCH: You will have extra time. You will have extra time.

SEN. SESSIONS: The attorney general explained that when I asked him. He narrowed my question when I raised it and made that qualification. Perhaps you weren't here when he did that.

SEN. FEINSTEIN: Right.

And Mr. Attorney General, I'd also like -- it's my view that the briefings of the big eight essentially violate the law as well. I believe that is a second violation of law, because I believe that Section 502 of 5 USC 413(a)(1) and (2) and (b)(1) and (2) specifically say how the intelligence committee should be notified.

I was present in the intelligence committee in December of 2001 when this was considered. And Senator Graham was chairman of the committee. And the committee really wanted all sensitive intelligence reported in writing, and what this did was set up a mechanism for that.

So, in my view, it was very clear that what the intelligence committee wanted at that time was all sensitive intelligence outside of covert to be reported to the committee, and this set up the format.

Now let me just move on, if I can.

ATTY GEN. GONZALEZ: Senator, can I respond to that?

SEN. FEINSTEIN: Sure. Sure, of course.

ATTY GEN. GONZALEZ: Because I disagree. First of all, both Chairman Roberts and Chairman Hoekstra disagree. They believe that we have provided notice as required by the law to the intel committees. And they both take the position that nowhere in the law does it require that each individual member of the intel committee be briefed.

The section that you provided that I think you quoted to -- and I must tell you, sometimes it gets kind of confusing to read these (B)(b)s and 1-1s; it gets kind of confusing. I think you are referring to a section which imposes an obligation on the president to ensure that agencies within the administration meet the notice requirements.

If you go to the actual notice requirements, however, under 413(A)(a), and 413(B)(b), those impose the obligations

to provide -- to make sure that the intel committees are currently and fully informed.

However, (A)(a), which deals with non-covert action, and (B)(b) which deals with covert action, both have a proviso that to the extent it doesn't it doesn't mean compromising -- and I'm paraphrasing here -- sources and methods and especially sensitive matters. So I think we've been acting consistent with the law, based upon these provisions that I just recited to you. There has been a long practice of giving briefings only to the chair and ranking or the certain limited subset of the intel committees.

And again, I would just simply remind the chairman that -- I mean remind the senator. Chairmen, I know, guard their prerogatives jealously. And both the chairman of the intel committee, Senate and House -- both chairmen have said we have met our obligations to provide briefings to the intel committee.

SEN. FEINSTEIN: Well, my reading of the law -- I disagree. I still disagree. I recognize we have a difference of opinion. I will propose an amendment to strengthen it in the next authorization bill. To me, and I remember being there -- I remember the discussion.

Anyway, I'd like to move on. I am puzzled, and I want to go back to why you didn't come for a change in FISA. Let me just read off a few of the changes that we have made to FISA. We extended the emergency exemption from 24 to 72 hours. We lowered the legal standard for surveillance to the significant purpose test. We allowed for John Doe roving wiretaps. We lowered the standard for FISA pin traps. We expanded their scope to include Internet routing information. We extended the scope of business records that can be sought under FISA. We extended the duration of FISA warrants. We broadened FISA to enable the surveillance of lone-wolf terrorists. And we made the director of national intelligence the lead authority.

Now, in view of the changes we have made, I cannot understand why you didn't come to the committee, unless the program was much broader and you believed it would not be authorized. That is the only reason I can figure you didn't come to the committee. Because if the program is as the president has said and you have said, to this date, you haven't briefed the intelligence committee; you haven't let us ask the question, what is a link? What is an affiliate? How many people are covered? What are the precise -- and I don't believe in the briefings those questions were asked -- what are the precise numbers? What happens to the data? How long is it retained in the database? When are innocent people taken out of the database?

I can only believe, and this is my honest view, that this program is much bigger and much broader than you want anyone to know.

ATTY GEN. GONZALEZ: Well, Senator, of course I cannot talk about aspects that are beyond what the president has already confirmed. What I can say is that those members of Congress who have received briefings know -- I think they know -- of course, I don't know what they actually know, but they have been briefed on all the details about all the activities. So they know what's going on.

SEN. FEINSTEIN: I understand your point of view.

Let me go to -- this morning I asked you whether there was any supreme case -- this goes to precedent -- that has held that the president can wiretap Americans since the Congress passed the FISA law. And you responded In re: Sealed case.

ATTY GEN. GONZALEZ: Which, of course, is not a Supreme Court case.

SEN. FEINSTEIN: That's right. I was going to bring that -- which is not a Supreme Court case.

ATTY GEN. GONZALEZ: I apologize if I was unclear.

SEN. FEINSTEIN: I just wanted to come back at you.

ATTY GEN. GONZALES: Yes, ma'am.

SEN. FEINSTEIN: So it is pure dicta, and --

ATTY GEN. GONZALES: It was not -- absolutely --

SEN. FEINSTEIN: I want to go back to the question that you might not like, but I'm going to ask it anyway: At the time of the In re: Sealed Case, did the Department of Justice or other administration officials tell the FISA court that warrantless domestic electronic wiretapping was going on?

ATTY GEN. GONZALEZ: At the -- in connection with that litigation, not to my knowledge, Senator.

SEN. FEINSTEIN: Okay. And since the passage of FISA, has any court spoken specifically to the president's authority to conduct warrantless domestic electronic surveillance?

ATTY GEN. GONZALEZ: Since the passage of FISA, a Supreme Court -- the Supreme Court -- I do not believe so. I think the last word on this by the Supreme Court is the Keef (sp) case, the 1972 case -- and I think that year is right. And there the court dealt with domestic security surveillance. And the court was very clear -- went out of its way, I believe, to make it clear that they were not talking about electronic surveillance for foreign intelligence purposes.

SEN. FEINSTEIN: Was the program mentioned to the court in the Hamdi case?

ATTY GEN. GONZALEZ: I do not know the answer to that question, Senator.

SEN. FEINSTEIN: I'd appreciate it if you could find the answer and let us know.

SEN. HATCH: Senator, take another two minutes because of our interruptions.

SEN. FEINSTEIN: Oh, thank you very much.

This morning you said, and I quote: "Presidents throughout our history have authorized the warrantless surveillance of the enemy during wartime, " end quote. Has any president ever authorized warrantless surveillance in the face of a statute passed by the Congress which prohibits that surveillance?

ATTY GEN. GONZALEZ: I think, actually, I think there was a statute on the books in connection with the order by President Roosevelt. I want to confirm that, but it is my recollection that that is in fact the case, that even though there was a statute on the books -- and maybe even a Supreme Court case; I can't remember now -- President Roosevelt ordered electronic surveillance.

SEN. FEINSTEIN: I'd be very interested to know that. If I understand your argument, it's that if one doesn't agree that the resolution to authorize military force provides a statutory exception to FISA, then FISA is unconstitutional.

ATTY GEN. GONZALEZ: No -- well, if that's the impression I gave, I don't want to leave you with that impression. That tees up, I think, a difficult constitutional issue.

I think the -- it's an easier issue for the executive branch side than the facts that were dealt with under Youngstown v. Sawyer because there you were talking about the president of the United States exercising dominion over part of our domestic industry, the steel industry.

Here you're talking about what I think is a much more core constitutional right of the commander in chief. I believe that the president -- that a statute that would infringe upon that I think would have some -- there would be some

serious constitutional questions there.

But I'm not prepared at this juncture to say absolutely that if our AUMF argument doesn't work here that FISA is unconstitutional as applied. I'm not saying that.

SEN. FEINSTEIN: You sidestepped FISA using the plenary authority as the commander in chief. The problem there as I see it is that section -- Article I Section 8 gives the Congress the authority to make the regulations for the military.

NSA is part of DOD; therefore, the Congress has the right to make those regulations.

ATTY GEN. GONZALES: I think that the clause you're referring to is the clause in Section 8 of Article I which clearly gives to the Congress the authority and power to make rules regarding the government and regulation of our armed forces.

And then the question is well, is electronic surveillance. Is that part of the government and regulation of our armed forces? There are many scholars who believe that there we're only talking about through the internal administration of our military, like court martials, like Selective Service.

And so I think there would be a question, a good debate and discussion about whether or not -- what does that clause mean and does it give to the Congress under the Constitution the authority to impose regulations regarding electronic surveillance?

I'm not saying that it doesn't. I'm just saying that I think that's obviously a question that would have to be resolved.

SEN. HATCH: Senator, your time is up.

Senator Grassley?

SEN. FEINSTEIN: Thank you. Thank you, Mr. Attorney General.

SEN. CHARLES GRASSLEY (R-IA): Thank you.

It appears to me that FISA generally requires that if surveillance is initiated under the emergency authorization provisions and an order is not obtained from the FISA court, that the judge must, quote, "cause to be served on any U.S. person named in the application and on such other U.S. persons subject to electronic surveillance as the judge and the court both believes warranted."

The fact of the application, two the period of the surveillance and three the fact that during the period information was or was not obtained.

So that brings these questions if that is the factual reading of the statute.

Does this explain the caution and the care and the time that is used when deciding whether to authorize 72-hour emergency surveillance?

And let me follow up. And then the possibility that if you got it wrong, could you wind up tipping off an enemy, in this case we're worried about al Qaeda terrorists?

Would this interfere with the president's ability to establish this vital early warning system under FISA?

And is this one of the reasons then, and this is the last question, is this one of the reasons why FISA is not as nimble and quick a tool as you need to combat terrorist threats and that members of this committee think ought to be used to a

greater extent?

ATTY GEN. GONZALES: Senator, those are all very, very good questions.

The reason we're careful about our work in seeking a FISA is because we want to get it right. We absolutely want to get it right in every case and we have career professionals working hard on these kinds of issues and we want to get it right.

It is true that if I authorize an emergency -- if I give an emergency authorization and an order is not obtained, my reading of the statute, my understanding of the statute is that the presumption is that the judge will then notify the target of that surveillance during that 72-hour period.

We would have the opportunity to make arguments as to why the judge should not do that, but in making those arguments, we may have to disclose information, certainly to the target. And if we fail, the judge may very well notify the target that they were under surveillance.

And if we fail, the judge may very well notify the target that they were under surveillance. And that would be damaging. That could possibly tip off a member of al Qaeda or someone working with al Qaeda that -- and we have reason to be concerned about their activities.

And so it is one of the many reasons why we take such great care to ensure that when I grant an emergency authorization that all the requirements of FISA are met.

The reason we have such a high approval rate at the FISA court is not because the FISA court is a rubber stamp. It's because we do our work at ensuring that those applications are going to meet the requirements of the statute.

SEN. GRASSLEY: What we know about al Qaeda and their method of operation, which I think at the very least we think that they -- involves the placement of sleeper cells in our country for months or -- they look way ahead; it could even be for years for a planned attack.

And the need to rely upon electronic communication network to convey instructions to those cells from command structures that would be located for al Qaeda outside the country. The surveillance program authorized by the president was tailored precisely to meet the natures of the threat that we face as a nation, particularly with sleeper cells.

Would that be right?

ATTY GEN. GONZALES: It is a narrowly-tailored program and, of course, that helps us in the Fourth Amendment analysis as to whether or not are these reasonable searches. And we believe that under the special needs jurisprudence, given the fact that we have been attacked from folks from al Qaeda within our country, we believe that these would satisfy the requirements of the Fourth Amendment.

SEN. GRASSLEY: I think in your opening statement, didn't you make a reference to bin Laden about his recent speech two weeks ago? And that's obviously a reiteration of the threat and he said that these attacks, future attacks, could dwarf the 9/11 magnitude.

If that is true, is it in some sense incredible to you that we're sitting here having this discussion today about whether the president acted lawfully and appropriately in authorizing a program narrowly targeted at communication that could lead, well lead, to a disruption or a prevention of such an attack?

ATTY GEN. GONZALES: Senator, I think that we should all be concerned to ensure that all branches of government are operating within the limits of the Constitution. And so I certainly -- I can't disagree with this hearing and the discussions, the questions in these hearings.

I think we have a good story to tell from the administration viewpoint. I wish there were more that we could tell because it's not simply a coincidence that the United States of America has not been hit again since 9/11. It's because of the brilliant and wonderful work of our men and women in the military overseas. It's because of tools like the Patriot Act. It's because of tools like the terrorist surveillance program.

SEN. GRASSLEY: Howard Dean, the chairman of the Democratic Party, was quoted recently as equating the terrorist surveillance program authorized by President Bush to, quote, "abuses of power during the dark days of the Nixon administration."

You're awful young, but does that have a fair comparison to you? And if it isn't a fair comparison, why or why not?

ATTY GEN. GONZALES: Well, it is not a fair comparison. I would direct you and the other members of the committee to Chairman Roberts' response to Mr. Dean in terms of making it clear that what's going on here is much more a kin to the directive by President Roosevelt to the Attorney General Jackson in terms of authorizing the department to -- authorizing his administration to initiate warrant-less surveillance of the enemy.

And so this is, again, this is not domestic surveillance. This is not going after our political enemies. This is about international communications. This is about going after al Qaeda.

SEN. GRASSLEY: I wonder if you'd discuss the nature of the threat posed by al Qaeda to our country because al Qaeda operates not under the rules of law, but disregard and contempt for conventional warfare.

In combating al Qaeda, can we afford to rely purely upon conventional law enforcement techniques, such as those traditionally used to combat organized crime groups or narcotic traffickers?

And if we were to do that, what would be the result?

ATTY GEN. GONZALES: The president expects us to use all the tools available under the Constitution. Obviously, we have strong law enforcement tools that we have been using and will continue to use.

But this is also a very serious military campaign and we're going to exercise and use all the tools, again, that are available to us in fighting this new kind of threat and this new kind of war.

SEN. GRASSLEY: I think we had some discussion from you about the review that goes on every 45 days, or approximately every 45 days. But the president himself said, quote, "carefully reviewed approximately every 45 days to ensure its ongoing propriety."

The surveillance is then re-authorized only after the president signs off on it. So I want to ask you a few questions about this review process. I want to ask these questions because it's important that the American people know whether the president has instituted appropriate procedures to guard against abuses.

Is the justice -- in the 42-page legal memorandum from your department, it's noted about the program, quote, "reviewed for legality by the Department of Justice and are monitored by the general counsel and the inspector general of the NSA to ensure that civil liberties are being protected."

I'd like to give you the opportunity to explain to the fullest extent possible -- without compromising the programs, the whats, who, when, why, where and how -- the period review.

What can you tell us about the periodic review and reauthorization of the surveillance program?

What assurances can you give the American people about their constitutional rights being zealously guarded against abuses?

ATTY GEN. GONZALES: There's a lot there in that question, Senator. I will do my best to respond.

Obviously, this is a periodic review approximately every 45 days or so. And we have people from the intelligence community evaluate whether or not al Qaeda -- what is the level of threat that continues to be posed by al Qaeda?

And during that period of time, we have monthly meetings out at NSA where people who are involved in the program, senior officials, they get together, sit down, talk about how the program is operating, ensuring that the program is being operated in a way that's consistent with the president's authorization.

In connection with each authorization, the department does make an analysis with respect to the legal authority of the president of the United States to move forward. And so there are administration lawyers that are involved looking to see whether or not does the president still have the authority to authorize the terrorist surveillance program that I've described here today.

SEN. GRASSLEY: I think my time's up. I was going to have some follow up questions on that point, but if it's necessary I'll submit it for answer in writing.

SEN. HATCH: Thank you, Senator.

Senator Feingold?

SEN. RUSSELL FEINGOLD (D-WI): Thank you, Mr. Chairman.

General Gonzales, when my time ended last time we were beginning to talk about the president's statements in the state of the union that his predecessors used the same legal authority that he is asserting.

Let me first ask do you know of any other president who has authorized warrant-less wiretaps outside of FISA since 1978 when FISA was passed?

ATTY GEN. GONZALES: None come to mind, Senator, but maybe I'd be happy to look to see whether or not that's the case.

SEN. FEINGOLD: Think it is a no unless you submit something.

ATTY GEN. GONZALES: I can't answer that I -- I can't give you an answer.

SEN. FEINGOLD: Okay. Isn't it true that the only federal courts to decide the president's authority to authorize warrant-less national security wiretaps were considering wiretaps carried out before the enactment of FISA?

ATTY GEN. GONZALES: I'm sorry, Senator. I was thinking about your question and I --

SEN. FEINGOLD: Would you like to answer the previous question?

ATTY GEN. GONZALES: No, but I was thinking about -- I was trying to think of an answer and I didn't catch the first part of your second question.

SEN. FEINGOLD: Isn't it true that the only federal courts to decide the president's authority to authorize warrant-less national security wiretaps were considering wiretaps that were carried out before the enactment of FISA?

ATTY GEN. GONZALES: In which there were actual decisions? Actually, there was a Fourth Circuit decision, the Truong decision, which was decided after FISA.

To be fair, I don't think they really got into an analysis.

SEN. FEINGOLD: That case was about a Vietnam era wiretap before FISA was enacted, right?

ATTY GEN. GONZALES: I believe -- the collection occurred before FISA was enacted. The decision was made after FISA and consequently, my recollection is is that case doesn't really get into a discussion about how the passage of FISA impacts or affects the president's --

SEN. FEINGOLD: If it was based on facts prior to FISA, then the only law that controls if the prior to FISA, right?

ATTY GEN. GONZALES: That's right. And then, of course, In re: Sealed Case, that did not --

SEN. FEINGOLD: You covered that with Senator Feinstein. That was dicta, correct?

ATTY GEN. GONZALES: Yes.

SEN. FEINGOLD: Thank you. So when the president said that federal courts have, quote, "approved the use of that authority," unquote, that he was trying to make people think that the courts had approved the authority he is invoking and the legal theory that you've put forward here.

That isn't really accurate, is it?

ATTY GEN. GONZALES: The president was totally accurate in saying that in considering the question as to whether or not the president has inherent constitutional authority to authorize warrant-less searches consistent with the Fourth Amendment to obtain foreign intelligence, the statement I think is perfectly accurate.

But he said that federal courts had said it was all right.

ATTY GEN. GONZALES: That's right.

SEN. FEINGOLD: And you aren't able to give me anything here since FISA that indicates that.

ATTY GEN. GONZALES: But Senator, I don't believe that he was making a statement since or before FISA. He was making the statement the courts who have considered the president's inherent constitutional authority had -- the court of appeals had said and I think there is -- in fact, there are five court of appeals decisions cited in the In re: Sealed Case.

All of them have said, I believe, that the president does have the constitutional authority to engage in this kind of surveillance.

SEN. FEINGOLD: Attorney General, that's why we just went over all this, because all of that is based on pre-FISA law. And here's my concern -- the president has somehow suggested that he couldn't wiretap terrorists before he authorized this program. He said, quote, "If there are people inside our country who are talking with al Qaeda we want to know about it." Unquote. And of course, I agree with that 100 percent and we have a law that permits it.

Isn't it true that FISA permits the NSA to wiretap people overseas without a court order, even if they call into the United States?

ATTY GEN. GONZALES: Well, of course, it depends.

SEN. FEINGOLD: Well, it does do that in some circumstances, does it not?

ATTY GEN. GONZALES: It could do it in some circumstances, depending on whether or not it is an electronic surveillance as defined under FISA. As you know, it is a very -- I don't want to say convoluted -- it's a very complicated definition of what kind of radio or wire communications would in fact be covered by FISA.

SEN. FEINGOLD: Attorney General, I understand that. But clearly, FISA, in part, does permit that kind of activity in certain cases.

ATTY GEN. GONZALES: Depending on the circumstances.

SEN. FEINGOLD: To leave the impression that there is no law permitting that would be incorrect.

ATTY GEN. GONZALES: Oh, of course not. We use FISA whenever we can.

SEN. FEINGOLD: -- trying to get at is the impression that the president left, I think, in the State of the Union was not completely accurate. Isn't it true that FISA permits the FBI to wiretap individuals inside the United States who are suspected of being terrorists or spies so long as the FBI gets secret approval from a judge?

ATTY GEN. GONZALES: Senator, I think I've already said that with respect to even domestic communication involving members of al Qaeda we use all the tools available to us including FISA. If we can get a FISA --

SEN. FEINGOLD: So the fact is, when the president suggests that he doesn't have that -- that power doesn't exist -- that power does exist, at least in part, under FISA -- under current law.

ATTY GEN. GONZALES: Well, Senator, I don't know whether or not that's what the president suggested, but clearly, the authority does exist for the FBI, assuming we can meet the requirements of FISA, assuming it is electronic surveillance covered by FISA to engage in electronic surveillance of al Qaeda here in this country.

SEN. FEINGOLD: Here's what the president said, he said, again quote, "If there are people inside our country who are talking with al Qaeda, we want to know about it." Unquote. I was sitting in the room. He sure left me the impression that he was suggesting that without this NSA program, somehow he didn't have the power to do that. That's misleading. So when the president said that he authorized a program to, quote, "Aggressively pursue the international communications of suspected al Qaeda operatives and affiliates to and from America -- trying to suggest that without this program he could not do that under the law -- that's not really right, is it?

ATTY GEN. GONZALES: Senator, I believe that what the president has said is accurate, is not misleading. We've -- the day following the New York Times story, he came out to the American people and explained what he had authorized. We had given numerous briefing to Congress since that day. I'm here today to talk about the legal authority for this program.

SEN. FEINGOLD: Well, I think the president's comments in the State of the Union were highly misleading. The American people need to know that you already have legal authority to wiretap anyone you suspect of helping al Qaeda and every person on this committee in this Senate supports your use of FISA to do just that.

Let me switch to another subject. Senator Feinstein sort of got at this, but I want to try a different angle. If you could answer this with a yes or no, I would obviously appreciate it. Has the president taken or authorized any other actions -- and other actions that would be illegal if not permitted by his constitutional powers or the authorization to use military force?

ATTY GEN. GONZALES: Repeat your question, please, Senator.

SEN. FEINGOLD: Has the president taken or authorized any other actions that would be illegal if not permitted by his constitutional powers or the authorization to use military force?

ATTY GEN. GONZALES: You mean in direct contradiction of the statute and relying upon his commander in chief authority?

SEN. FEINGOLD: Has he taken any other actions -- yes, that would be illegal --

ATTY GEN. GONZALES: Not to my knowledge, Senator.

SEN. FEINGOLD: In other words, are there other actions under the use of military force for Afghanistan resolution that, without the inherent power, would not be permitted because of the FISA statute? Are there any other programs like that?

ATTY GEN. GONZALES: Well, I guess what I'd like to do, Senator, is I want to be careful about answering your question. I obviously cannot talk about operational matters that are not before this committee today and I don't want to leave you with the wrong impression. And so I would like to get back to you with an answer to your question.

SEN. FEINGOLD: I definitely prefer that to then being told that something's a hypothetical.

On September 10, 2002, Associate Attorney General David Criss (sp) testified before the Senate Judiciary Committee. His prepared testimony includes the following statement, quote, "Thus both before and after the Patriot Act, FISA can be used only against foreign powers and their agents and only where there is at least a significant foreign intelligence purpose for the surveillance." Let me repeat for emphasis: "We cannot monitor anyone today whom we could not have monitored at this time last year." Unquote. And this last sentence was actually underlined for emphasis in the testimony, so let me repeat it too -- "We cannot monitor anyone today whom we could not have monitored at this time last year."

Now I understand that Mr. Criss (sp) did not know about the NSA program and has been highly critical of the legal justifications offered by the Department. I also realize that you were not the attorney general in 2002. So I know you won't know the direct answer to my question, but can you find out -- and I'd like if you can get me a response in writing -- who in the White House and the Department of Justice reviewed and approved Mr. Criss's (sp) testimony? And of those people, which of them were aware of the NSA program and thus let what was obviously a highly misleading statement be made to the Congress of the United States? Will you provide me with that information?

ATTY GEN. GONZALES: We'll see what we can provide to you, Senator. Sir, my understanding is that Mr. Criss (sp) -- I don't think it's fair to characterize his position as highly critical. I think he may disagree, but saying it's highly critical, I think, is unfair.

SEN. FEINGOLD: Well, we can debate that, but the point here is to get to the underlying information. I appreciate your willingness to get that for me if you can.

General Gonzales, I'd like to explore a bit further the role of the telecommunications companies and Internet service providers in this program. As I understand it, surveillance often requires the assistance of these service providers and the providers are protected from criminal and civil liability if they've been provided a court order from the FISA court or criminal court or if a high ranking Justice Department official has certified in writing that, quote, "No warrant or court order is required by law, that all statutory requirements have been met and that the specified assistance is required." Am I accurately stating the law?

ATTY GEN. GONZALES: I believe that's right, Senator.

SEN. FEINGOLD: Have you or anyone at the Justice Department provided any telephone companies or ISP's with these certifications in the course of implementing the NSA's program?

ATTY GEN. GONZALES: Sir, that is an operational detail that I just can't go into in this hearing.

SEN. FEINGOLD: I look forward to an opportunity to pursue it in other venues and thank you very much.

ATTY GEN. GONZALES: Thank you, Senator.

SEN. HATCH: Thank you, Senator.

Senator Kyl.

SEN. JON KYL (R-AZ): Thank you, Mr. Chairman. I hadn't intended to ask any questions, but I think there are two areas that need to be cleared up.

First, with regard to two points that Senator Feingold said the president -- in which the president made highly misleading statements -- one in the State of the Union, allegedly leaving the impression that the president had authority he didn't have. When he discussed the president, the authority that he had that other presidents had or had exercised, what was he referring to there? Was he referring to FISA or was he referring to something else?

ATTY GEN. GONZALES: Senator, he was referring to the president's inherent constitutional authority to engage in electronic surveillance of the enemy.

SEN. KYL: Exactly. And secondly, Senator Feingold asked you if there was authority under FISA to conduct wiretaps, including of suspected al Qaeda terrorists and it was misleading for the president to infer otherwise. Is it possible to acknowledge that FISA authority exists, while also making the point that it's not the optimal or maybe even workable method of collection of the kind that's done under the surveillance program at issue here?

ATTY GEN. GONZALES: No question about it. It is one of the reasons for the terrorist surveillance program is that while FISA ultimately may be used, it would be used in a way that's ineffective because of the procedures that are in FISA.

SEN. KYL: Thank you.

Now, let me clear up a concern expressed by Senator Feinstein that the reason that Congress hadn't been asked to statutorily authorize this surveillance program may be because it's much bigger than we have been led to believe. Is that the reason?

ATTY GEN. GONZALES: Senator, the reason is because, quite frankly, we didn't think we needed it under the Constitution. And also because we thought we had it with respect to the action by the Congress. We have believed from the outset that FISA has to be read in a way which is not inconsistent with the president's constitutional authority as commander in chief.

SEN. KYL: Right. Now, there was also discussion about briefings by the intelligence community -- General Hayden and perhaps others -- to what's been the called the Big Eight, which are the four elected leaders, bipartisan, of the House and Senate and the four chairman and ranking member of the two committees -- of the two intelligence committees of the Congress.

Was that the group that you referred to when you said that there had been discussion about whether to seek an amendment of FISA in the Congress?

ATTY GEN. GONZALES: Senator, it included the leadership of the Congress and the leadership of the intel committees.

SEN. KYL: Okay. And in terms of evaluating -- there was also, Senator Leahy asked the question about why you didn't come to members of this committee. Who would be in a better position to judge or to assess the impact on our intelligence with respect to compromise of the program? Would it be the leadership and chairman and ranking members of the intelligence committees or members of this committee that haven't been read into the program?

ATTY GEN. GONZALES: Sir, the judgement was made that the conversation should occur with members of the intel committee and the leadership of the Congress bipartisan.

SEN. KYL: And in fact, if you came to this committee to seek amendments to cover the program at issue, the

members of this committee would have to be read into the program, would they not?

ATTY GEN. GONZALES: Yes, sir.

SEN. KYL: Senator Leahy also said, thank goodness -- I'm paraphrasing now -- thank goodness that we have the press to tell us what the administration's doing with this program because we wouldn't know otherwise.

And of course, the press did disclose the existence of this highly classified program, which you have indicated has compromised the program to some extent or has done damage to it -- I forgot your exact phrase.

ATTY GEN. GONZALES: Those, I believe, were the comments from the CIA director.

SEN. KYL: All right. And it seems to me, Mr. Chairman, that the attitude that it's a good thing that this program was compromised validates the view of the bipartisan leadership that briefing members of Congress further -- or at least briefing members of this committee -- would further jeopardize the program.

It seems to me that those entrusted with knowledge of this program must be committed to its protection.

Thank you, Mr. Chairman.

SEN. HATCH: Thank you, Senator.

Senator Schumer.

SEN. CHARLES SCHUMER (D-NY): Thank you, Mr. Chairman.

I just want to go back to where we left off and then I'll move forward. And thank you, General Gonzales. I know it's been a long day for you -- especially with all that bobbing and weaving, it's not so easy.

We talked before about the legal theory that you have under AUMF. And I had asked you that under your legal theory can the government without ever going to a judge or getting a warrants, search an American's home or office? I'm not saying -- well, can you give me an answer to that? Why wouldn't the same exact legal theory apply -- that the Congress in the resolution gave the president power he needed to protect America. Why is one different than the other -- both are fourth amendment?

ATTY GEN. GONZALES: I'm not suggesting that it is different. Quite frankly, I would like the opportunity simply to --

SEN. SCHUMER: I'm sorry, if you could pull the mike --

ATTY GEN. GONZALES: I'm not saying that it would be different. I would simply like the opportunity to contemplate over it and give you an answer.

SEN. SCHUMER: And you will be back here, though, so we can ask that, right?

ATTY GEN. GONZALES: According to the chairman.

SEN. SCHUMER: Okay, good. If not, I would ask unanimous consent that Mr. Gonzales -- General Gonzales -- be given time to answer that one in writing.

SEN. HATCH: He said he will.

SEN. SCHUMER: Okay, good. Now, here's the next question I have -- has the government done this? Has the government searched someone's home -- and American citizen or office -- without a warrant since 9/11, let's say?

ATTY GEN. GONZALES: Sir, to my knowledge, that has not happened under the terrorist surveillance program and I'm not going to go beyond that.

SEN. SCHUMER: Wait, I don't know what that -- what does it mean, under the terrorist surveillance program? The terrorist surveillance program is about wiretaps. This is about searching someone's home. It's different. So it wouldn't be done under the surveillance program. I'm asking you, has it been done? ATTY GEN. GONZALES: But now you're asking me questions about operations or possible operations and I'm not going to get into that, Senator.

SEN. SCHUMER: I'm not asking you about any operation. I'm not asking you how many times, I'm not asking you where.

ATTY GEN. GONZALES: You asked me, has that been done.

SEN. SCHUMER: Yes.

ATTY GEN. GONZALES: Have we done something?

SEN. SCHUMER: Yeah.

ATTY GEN. GONZALES: That is an operational question in terms of how we're using our capabilities.

SEN. SCHUMER: Okay, so you won't answer whether it is allowed and you won't answer whether it's been done. I mean, isn't part of your -- in all due respect, as somebody who genuinely likes you -- but isn't this part of your job to answer a question like this?

ATTY GEN. GONZALES: Of course it is, Senator, and --

SEN. SCHUMER: But you're not answering it.

ATTY GEN. GONZALES: Well, in fact, I'm not saying that I will not answer the question.

SEN. SCHUMER: Oh.

ATTY GEN. GONZALES: I'm just not prepared to give you an answer at this time.

SEN. SCHUMER: Okay, well, all right. I'll accept.

And I have another one and we can go through the same thing. How about wiretap under the illegal theory, can the government without ever going to a judge wiretap purely domestic phone calls?

ATTY GEN. GONZALES: Again, Senator, give me an opportunity to think about that, but of course, that is not what this program is.

SEN. SCHUMER: It's not -- I understand. I'm asking because under the AUMF theory you are allowed to do it for these wiretaps, I just want to know what's going on now. Let me just -- has the government done this? You can get back to me in writing.

ATTY GEN. GONZALES: Thank you, Senator.

SEN. SCHUMER: Okay, and one other, same issue -- placed a listening device -- has the government without ever going to a judge placed a listening device inside an American home to listen to the conversations that go on there? Same answer?

ATTY GEN. GONZALES: Same answer, Senator.

SEN. SCHUMER: Okay, but now I have another one and let's see if you give the same answer here. And that is, under your legal theory, can the government without going to a judge -- this is legal theory, I'm not asking you whether they do this -- monitor private calls of its political enemies? People not associated with terrorists, but people who they don't like politically?

ATTY GEN. GONZALES: We're not going to do that. That's not going to happen.

SEN. SCHUMER: Okay. Next, different issue. Last week in the hearing before the Intelligence Committee, General Hayden refused to state publicly how many wiretaps have been authorized under this NSA program since 2001. Are you willing to answer that question -- how many have been authorized?

ATTY GEN. GONZALES: I cannot -- no, sir, I'm not at liberty to do that. I believe -- and of course, I have not been at all the briefings for the congressional leaders and the leaders of the intel committee. I believe that that number has been shared, however, with members of Congress.

SEN. SCHUMER: You mean the chair of the Intelligence Committee or something?

ATTY GEN. GONZALES: I --

SEN. SCHUMER: It's not a classified number, is it?

ATTY GEN. GONZALES: It is a classified -- I believe it is a classified number, yes, sir.

SEN. SCHUMER: But here's the issue -- FISA is also important to our national security and you praise the program, right?

ATTY GEN. GONZALES: I couldn't agree with you more, Senator.

SEN. SCHUMER: Okay.

ATTY GEN. GONZALES: It's very important.

SEN. SCHUMER: Now, FISA makes public every year the number of applications. In 2004, there were 1,758 applications. Why can't we know how many under this program? Why should one be any more classified than the other?

ATTY GEN. GONZALES: I don't know whether or not I have a good answer for you, Senator.

SEN. SCHUMER: I don't think you do.

ATTY GEN. GONZALES: The information is classified, and I would not be at liberty to talk about it here in this public --

SEN. SCHUMER: And I understand this isn't exactly your domain, but can you -- I can't even think of a rationale why one should be classified and one should be made routinely public. Both involve wiretaps, both involve terrorism, both involve protecting American security, and we've been doing the FISA one all along. I'm sure -- well, let me ask you this, if the administration thought that revealing the FISA number would damage security, wouldn't they move to classify it?

ATTY GEN. GONZALES: Maybe -- of course now I'm just -- I'm going to give you an answer. Perhaps it has to do with the fact that with FISA, of course, it's much, much broader. We're talking about enemies beyond al Qaeda. We're talking about domestic surveillance. We're talking about surveillance that may exist in peacetime, not just in war time. And so, perhaps, the equities are different in making that information available to Congress.

SEN. SCHUMER: Would you support declassifying that number?

ATTY GEN. GONZALES: Senator, I would have to think about that.

SEN. SCHUMER: We'll wait for the next -- (inaudible) -- another one. We have a lot of questions to follow up on here.

ATTY GEN. GONZALES: I look forward to our conversation.

SEN. SCHUMER: Me, too. Abuses -- this is -- when Frank Church was speaking at the hearing that Senator Kennedy, I think, talked about much earlier this morning, he said -- the NSA's quote-- "Capability at any time could be turned around on the American people and no American would have any privacy left, such as the capability to monitor everything -- telephone conversations, telegrams, it doesn't matter; there'd be no place to hide." Now it's 31 years later and we have even more technology, so there's the potential that Senator Church mentioned for abuse is greater.

So let me ask you these questions. I'm going to ask a few of them so you can answer them together.

Have there been any abuses of the NSA surveillance program? Have there been any investigations arising from concerns about abuse of the NSA program? Has there been any disciplinary action taken against any official for abuses of the program?

ATTY GEN. GONZALES: Senator, I think that --

SEN. SCHUMER: Because this gets to the nub of things. This is what we're worried about.

ATTY GEN. GONZALES: Of course.

SEN. SCHUMER: I think all of us want to give the president the power he needs to protect us. I certainly do. But we also want to make sure there are no abuses. And so if there have been some abuses, we ought to about, and it might make your case to say, yeah, we found an abuse or a potential abuse and we snuffed it out. Tell me what the story is.

ATTY GEN. GONZALES: Well, I do not have answers to all these questions. I'd like to remind people that, of course, in the area of criminal law enforcement, when you talk about probable cause, sometimes there are mistakes made, as you know.

SEN. SCHUMER: No question. No one's perfect.

ATTY GEN. GONZALES: The mistake has to be one that would be made by a reasonable man. And so when you ask have there been abuses, I can't -- these are all --

SEN. SCHUMER: Have there been any -- how about this --

ATTY GEN. GONZALES: Disciplinary action --

SEN. SCHUMER: Yeah, this is something that you ought to know, if there's been any disciplinary action, because I take it that would be taken --

ATTY GEN. GONZALES: Not necessarily. I think -- the NSA, I think, has a regimen in place where they ensure that people are abiding by agency policy in regulations.

SEN. SCHUMER: If I asked those two questions about the Justice Department, any questions arising out of concern for abuse of NSA surveillance or any disciplinary action taken against an official, in either case by the Justice department, you would know the answer to that.

ATTY GEN. GONZALES: I probably would know the answer to that. To my knowledge, then, no.

SEN. SCHUMER: Okay. Could you commit when we come back to tell us if there have been -- you know, you can then go broader than you know and then more broadly than what you --

ATTY GEN. GONZALES: In terms of what is going on at NSA, or Justice?

SEN. SCHUMER: NSA.

ATTY GEN. GONZALES: Well --

SEN. SCHUMER: I mean, as the chief law enforcement officer, it's still your job to sort of know what's going on in other agencies.

ATTY GEN. GONZALES: Sir, but if we're not talking about -- each agency has its own policies and procedures --

SEN. SCHUMER: Just asking you when you come back next time to try and find the answer --

ATTY GEN. GONZALES: I'll see what I can do about providing additional information to your questions.

SEN. SCHUMER: A little soft, but I'll have to take it, I guess.

Thank you, Mr. Chairman.

SEN. GRASSLEY: Thank you.

Senator DeWine.

SEN. MIKE DEWINE (R-OH): Thank you, Mr. Chairman.

Long day, Mr. Attorney General. Let me just you a few questions.

We've had a lot of discussions today, and you've referenced a lot to this group of eight, reporting to this group of eight. I just want to make a point; it's a small point, I guess. But the statutory authorization for this group of eight is 50USC413b. When you look at that section, the only thing this references, as far as what this group of eight does, is receive reports in regard to covert action. So that's really what all it is. There's no -- does not cover a situation like we're talking about here at all.

So I just wanted to make that point. We all have a great deal of respect of these eight people. It's a different group of eight in different periods of time. We've elected them. We've selected them. They are leaders of the Congress. But there's no statutory authority for this group other than this section that has to do with covert operation, and this is not a covert operation as defined in the specific section.

ATTY GEN. GONZALES: Senator, can I respond to you?

SEN. DEWINE: Sure.

ATTY GEN. GONZALES: Because I had a similar question from Senator Feinstein. I don't know whether or not you were here or not.

First of all -- again, repeating for the record that, of course, the chairman of the Senate intel committee and the chairman of the House intel committee --

SEN. DEWINE: And I was here when she --

ATTY GEN. GONZALES: Okay. They both have communicated that we are meeting our statutory obligations. There is a provision that requires the president of the United States to ensure that agencies are complying with their notice requirements. The actual notice requirements, as I read it, are 413(A)(a) and 413(B)(b). And 413(A)(a) deals with non-covert action; 413(B)(b) deals with covert action. And both of them --

SEN. DEWINE: Mr. Attorney General, I don't have much time. I don't mean to be impolite --

ATTY GEN. GONZALES: Okay. That's alright.

SEN. DEWINE: I listened to that and I respect your position on it. My only point was a small point.

ATTY GEN. GONZALES: Yes, sir.

SEN. DEWINE: And that point simply is that when we reference the group of eight, there's no statutory authorization for the group of eight other than for a covert operation. I guess I'm just kind of a strict constructionist, kind of a conservative guy, and that's how I read the statute. And that's my only point. And I understand your legal interpretation; I respect that. But you know, that's it. I don't see any other way on that.

Let me ask you a couple of other questions that I wonder if you could clarify for me. One is the legal standard that you are using, that's being used by the NSA under this program for deciding when to conduct surveillance of a suspected terrorist. In your December 19th press conference, you said you must have, and I quote, "reasonable basis to conclude that one party to the communication is affiliated with al Qaeda."

Speaking on Fox TV yesterday, General Hayden referred to the standard as "in the probable cause range." Could you define it for me? I know you talked about it today, but we're hearing a lot of different definitions.

ATTY GEN. GONZALES: To the extent there's --

SEN. DEWINE: You're the attorney general, and just clarify it for me, pinpoint it, give me a definition that the people who are administering this every single day in the field are following.

ATTY GEN. GONZALES: To the extent there's confusion, we must take some of the credit for the confusion, because we have used different words. The standard is a probable cause standard. It is reasonable grounds to --

SEN. DEWINE: A probable cause standard. Is that different than probable cause as we would normally learn at law school, or is there --

ATTY GEN. GONZALES: Not in my judgment.

SEN. DEWINE: Okay. So that means, I think, it's probable cause.

ATTY GEN. GONZALES: It's not probable cause as to guilt --

SEN. DEWINE: I understand.

ATTY GEN. GONZALES: -- or probable cause as to a crime being committed. It's probable cause that a party to the communication is a member or agent of al Qaeda. The precise language that I'd like you to refer to is, is there reasonable grounds to believe -- reasonable grounds to believe that a party to the communication is a member or agent of al Qaeda or of an affiliate terrorist organization? So it is a probable cause standard, in my judgment.

SEN. DEWINE: So probable cause.

ATTY GEN. GONZALES: It's probable cause.

SEN. DEWINE: And so all the case law or anything else that we would learn throughout the years about probable cause about that specific question would be what we would look at and what the people are being instructed to follow.

ATTY GEN. GONZALES: But again, it has nothing to do with probable cause of guilt, or probable cause that a crime had been committed --

SEN. DEWINE: I understand. We're extrapolating that traditional standard over to another question.

ATTY GEN. GONZALES: And the reason that we use these words instead of probable cause is because the people relying upon the standard are not lawyers.

SEN. DEWINE: Let me follow up. I don't have much time.

General Hayden described the standard as a softer trigger than the one that's used under FISA. What does that mean?

ATTY GEN. GONZALES: I think what General Hayden meant was that the standard is the same, but the procedures are different in that you have more procedures that have to be complied with under FISA. But the standards are the same in terms of probable cause. But there are clearly more procedures that have to be met under FISA, and that's what I believe General Hayden meant by the softer trigger.

SEN. DEWINE: So it's more -- it's a procedure issue then. In other words, I've got to go through more hoops on one, loops on the other. It's a difference what I have to go through, but my legal standard's the same. Is that what you're saying?

ATTY GEN. GONZALES: It's a probable cause standard for both. And yes, sir -- what has to --

SEN. DEWINE: It's the same standard.

ATTY GEN. GONZALES: It is the same standard.

SEN. DEWINE: Different question, but different procedures.

Final follow-up question on this. I believe you said that the individual NSA analysts are the ones who are making these decisions. People in the -- who are actually doing this or making this decision obviously -- what kind of training are these individuals given in regard to applying the standard? Well, are you involved in that, or are you not involved in that?

ATTY GEN. GONZALES: This is primarily handled by the general counsel's office at NSA, and, as you know, they are very, very aware of the history of abuses. They care very much about ensuring that all the activities that are ongoing at NSA are consistent with the Constitution, and certainly consistent with the authorization by the president for this terrorist surveillance program.

SEN. DEWINE: So this is not something your department is directly involved in?

ATTY GEN. GONZALES: No sir, I think it would be unfair to say that we are directly involved. We have provided some guidance, but I think it would be unfair to say that the Department of Justice has been intimately involved in providing training and guidance. I think it's fair to say that that responsibility has fallen primarily to the general counsel's office out at NSA.

SEN. DEWINE: Mr. Attorney General, I will conclude at this point. I just go back to what I said this morning, and that is, we've heard a lot of debate -- even more debate than we have this morning about these legal issues and people on different sides of these legal issues. I just really believe it's in the country's best interest, the president's best interest, the

war on terrorism's best interest, which is what we're all concerned about. Some four years or so after this program has been initiated, for the president to come to Congress and to get -- for us in the intelligence committee that has jurisdiction to take a look at this program, to get the briefing on the program and then see whatever changes in the law have to be made and to deal with it.

I think you will be, and the president will be in a much stronger position at this point to go forward, and it will be in the best interest of the country.

ATTY GEN. GONZALES: Thank you, Senator.

SEN. GRASSLEY: Thank you, Senator.

Senator Kennedy.

SEN. EDWARD KENNEDY (D-MA): Thank you, Mr. Chairman.

And thank you, General Gonzales. I join all of those that pay tribute to you for your patience on this, and thank you for responding to the questions.

Just to pick up on what my friend and colleague Senator DeWine has mentioned: I'm in strong agreement with -- that recommendation's bipartisan; I didn't have a chance to talk to Senator DeWine.

I mentioned earlier in the course of our visit this morning that we had, I thought, extraordinary precedents with Attorney General Levi, Ed Levi, and President Ford, where the members of this committee, a number of us went down to the Justice Department, worked with them. They wanted to get it right. The issue was on eavesdropping -- very related to the subject matter -- that they wanted to get it right. And then General Levi had a day and a half where he listened to outside constitutional experts, because he wanted to get it right.

My very great concern is that we're not getting it right. Maybe in terms of the NSA thinks that they're getting the information, but what we're seeing now with the leaks and others -- that there are many people out there that wonder whether they're going to face future prosecution, whether the court system's going to be tied up because of information that's gained as a result of the NSA taps that's not going to be permitted, and that we're going to have these known al Qaeda personnel that are going to be either freed or given a lesser sentence, or whatever, and that they're less inclined to sort of spill the beans, because if they know that they're going away, or worse, they'll be better prepared to make a deal with law enforcement authorities than if they think they can tie up the courts.

So in the FISA Act, as you well know, the 15 days that were included in there were included, as the legislative history shows; that if they needed to have a broader context, it was spelled out in the legislative history. The administration would have seven days, allegedly, to make emergency recommendations, and we'd have seven days to act. Maybe that was too precipitous, but that was certainly the intent -- the invitation of the time, to recognize the time. And I think I believe very strongly that that's, as Senator DeWine has made -- we want to get -- we have uncertainty now. When you have those within your own department who wonder about the legality, the list of constitutional authorities and question the legality. You have Professor Curtis Bradley, who'd been -- someone who'd been part of the administration. The State department questions the legality. I think we're -- this is a matter of concern.

I understand -- I asked you; I didn't think I gave you a chance to answer. But we -- you really didn't have a chance to test this out with outside constitutional authority, as I understand it.

ATTY GEN. GONZALES: Sir, of course I wasn't at the department when the program commenced, and so certainly, from within the White House, I'm not aware of any discussions, generally or specifically. I don't think there would have been any specific discussions with outside experts. And I suspect -- in fact, I'm fairly sure -- there were not discussions with outside expertise at the department, although I don't know for sure.

SEN. KENNEDY: Well, the -- we'll have our chance and opportunity, hopefully, to find that out. But it -- in further hearings. But it is impressive, but -- what was done previously and the coming together in -- when the legislation was passed, with virtually unanimity and in the House and the Senate. And I think that, as others have expressed, we want to give the president the power to get what's right in terms of protecting us, but we need, as we do on other issues, have the kinds of checks and balance to make sure that it's done right.

Let me just -- I have just a couple of other areas. I'm not sure that -- you might have been asked about this, and if you can't answer it, you can't answer. But since September 11th, has the president authorized any other surveillance program within the United States under his authority as commander in chief or under the authorization for use of military force in Afghanistan --

ATTY GEN. GONZALES: Senator, I'm not -- I can't answer that question in terms of other operations.

SEN. KENNEDY: Okay. All right.

On another issue -- and I've heard from staff, apologize for not being here through the whole session -- we were dealing with the asbestos legislation on the floor at the time, and I needed to go over to the floor -- I'm interested in the telephone companies that assist the government engaging in electronic surveillance, face potential criminal and civil penalties if they disclose consumer information unlawfully.

So they are protected from such liability if they receive a written certification from the attorney general or his designee, saying that -- and I quote -- "no warrant or court order is required by law, that all statutory requirements have been met, and that this specific assistance is required."

So you understand that telephone companies can face criminal and civil liability if they provide wiretapping assistance in a way that's not authorized by statute.

ATTY GEN. GONZALES: I do understand that, yes, sir.

SEN. KENNEDY: And have you provided a certification to the telephone companies that all statutory requirements have been met?

ATTY GEN. GONZALES: Senator, I --

SEN. KENNEDY: You can't answer that?

ATTY GEN. GONZALES: -- I can't provide that kind of information.

SEN. KENNEDY: And you couldn't even provide us with redacted copy. So I guess we'd assume that since that's a requirement or otherwise that they can be -- they'll be held under the criminal code, and that is a requirement, one would have to assume that you've given them that kind of authority by that --

ATTY GEN. GONZALES: Senator, two points.

There is a lot in the media about potentially what the president has authorized.

SEN. KENNEDY: Okay.

ATTY GEN. GONZALES: Much of it is incomplete. Much of it is, quite frankly, wrong. And so you have this muddled picture that the president has authorized something that's much greater than what in fact he has authorized.

And I can't remember my second point.

SEN. KENNEDY: But your response to the earlier question about the range of different programs --

ATTY GEN. GONZALES: Oh, I remember my second -- if I can just -- my second point is, is that your question -- again, I haven't -- I think this is true. I don't want to give -- well, maybe I shouldn't make this statement.

I'm sorry. Go ahead, Senator.

SEN. KENNEDY: Well, that's -- we were looking at sort of the range of different programs. But I think that there's -- I want to just mention, General, as someone that was here when we had the testimony -- just quickly -- on the wiretaps, there was -- prior to the time that J. Edgar Hoover used to appear, they used to lift all the wiretaps. They'd just have about 450 or 500 wiretaps, and they have 20 the day he testified, then 500 the next day. No one's suggesting that that's what's happening. But that's really what many of us who have been on this committee for some time have seen those abuses. No one is suggesting that. And we understand your reluctance in mentioning this. But we've -- this is an issue that's been around over some period of time.

I'd just say in conclusion, Mr. Chairman, I'm very hopeful. We want to have as much certainty on the program as possible. I think the -- what we have seen out in the public now is the information that has been out there almost -- certainly weekly, as a result of concerned individuals in these agencies, hard-working Americans that are trying to do a job and are concerned about the legality of this job. And I think they are entitled to the protections that we ought to be able to provide for them. And as someone who's been a member of this committee, I think that this committee has in the past, and certainly would, recognizing the extraordinary sensitivity and the importance of it, do the job and do it right and do it well. And then done so, I think we would have a different atmosphere and a different climate, and I think we'd be able to get the kind of information that is going to be so important to our national security. I hope that will be a judgment that you'll consider, as Senator DeWine has mentioned, and others have mentioned. And I appreciate your testimony.

Thank you, Mr. Chairman.

SEN. SPECTER: Before proceeding to Senator Sessions, who's next on the Republican side -- and I will defer my turn until after Senator Sessions has had his turn -- I think this is a good time to make an announcement.

Senator Kennedy made this suggestion earlier today about the committee's intentions with respect to renewing the Voting Rights Act; especially propitious time with the death of Coretta Scott King. We have been talking about hearings. And we're going to move to renew the Voting Rights Act this year, if we possibly can, in advance of the 2007 date. We have been laboring under a very, very heavy workload, which everybody knows about. And we will be scheduling those hearings early on. They have to be very comprehensive, provide an evidentiary base. And it is a matter of great concern really to everybody on the committee.

But, Senator Kennedy --

SEN. KENNEDY: Well, I want to thank the chair. We've had a chance to talk about this at other times. But that -- and I particularly appreciate his sensitivity as many of us are going down to the funeral for Coretta Scott King. I think it's an important statement and comment that her legacy will continue. So I thank -- I thank the chair.

I know we have broad support. My friend Senator Leahy has been a strong supporter, others here -- Senator Biden -- I look around this committee. It's very, very important legislation. In the time that we inquired of General Gonzales, he had indicated the full support of the administration on this. We'll look forward to working with you.

I thank the chair for making that announcement.

SEN. SPECTER: Thank you, Senator Kennedy.

Senator Sessions.

SEN. SESSIONS: Thank you, Mr. Chairman.

I would like to offer for the record a letter from Mr. H. Bryan Cunningham, who served for six years with the CIA and the Department of Justice in President Clinton's administration, and for a time in President Bush's administration, in which he defends the actions of the terrorist program -- surveillance program.

I would also join with the chairman in welcoming Ms. Debra Burlingame here. She's been here all day. Her brother was a pilot who lost his life in the plane that crashed into the Pentagon, and I think her presence today is a vivid reminder of the human cost that can occur as a result of negligence or failure of will, or failure to utilize the capabilities that are constitutional and are legal in this country.

And we have a responsibility to make sure that we do those things that are appropriate and legal to defend this country. It's not merely an academic matter. We've had some good discussions here today. But it's beyond academics. It's a matter of life and death, and we've lost a lot of people, over 300 -- nearly 3,000 people have no civil rights today. They're no longer with us as a result of a terrorist attack.

Thank you, Ms. Burlingame, for coming and being with us today.

We talked about the inherent power of the president. I think there's been a remarkable unanimity of support for the inherent power of the president to do these kind of things in the interest of national security, and I know post-Aldrich Ames, as you pointed out when I asked you about it, Mr. Gonzales, Attorney General Gonzales, that laws were changed with regard to that. But in fact, Jamie Gorelick, the deputy attorney general in the Clinton administration, testified before Congress in defense of an -- a warrantless search of Aldrich Ames's home and the warrantless search of a Mississippi home of a terrorist in the Aldrich Ames case.

She testified that the president has inherent authority to conduct warrantless physical searches for foreign intelligence purposes. Now, that sounds to me like that she was saying that that is an inherent constitutional power. I don't understand it any other way. Would you?

SEN. : Senator, yield for a question. What year was that? I'm sorry.

SEN. SESSIONS: This would have been after the Aldrich Ames case, `94-`95.

SEN. : Thank you.

SEN. SESSIONS: It was before the statute was changed by the Congress, but she did not discuss it in that context. Her context was that it's the inherent power of the president.

And she went on to say, "and the rules and methodologies for criminal searches are inconsistent with the collection of foreign intelligence and would unduly frustrate the president in carrying out his foreign intelligence responsibilities."

And in addition to that, Judge Griffin Bell, who served as a federal judge for a number of years and was attorney general under our Democratic President Jimmy Carter when the FISA act was passed, acknowledged that while the bill did not recognize the president's inherent power to conduct electronic surveillance, he said this, quote: This does not take away the power of the president under the Constitution. It simply, in my view, is not necessary to state that power, so there is no reason to reiterate or iterate it, as the case may be; it is in the Constitution, whatever it is.

And then he went on to say a little later -- when asked about the inherent power of the president to order electronic surveillance without first obtaining a warrant, former Attorney General Griffin Bell testified: We can't change the Constitution by agreement -- or by statute, I would add. A little later he said, when asked if he thought the president has, quote -- he was asked this question: Does the president have, quote, "the inherent right to engage in electronic

surveillance of an American citizen in this country?" Judge Bell responded: I do. I think he has a constitutional right to do that, and he has a concomitant constitutional duty to do it under certain circumstances.

So I don't know all the answers to what the powers are here. There are a lot of different opinions. I would say this. You've almost been criticized some today for not going further, not surveilling purely phone calls within our country. Some on the other side have criticized you, apparently, are surprised you didn't assert that authority. But the president, I think, acted narrowly and within what he thought would be appropriate given our constitutional and statutory structure and after having informed eight of the top leaders in the United States Congress. Would you comment on that?

ATTY GEN. GONZALES: Well, it is a very narrow authorization. And again, I want to repeat what I said earlier in the hearings in terms of I want to assure you that we -- that while domestic-to- domestic is not covered under the terrorist surveillance program, we are using all the tools available, including FISA, to get information regarding those kinds of communications. I mean, if there are other ways to do it that are permitted under the Constitution, we're going to try to get that information. It's so very, very important.

SEN. SESSIONS: Well, thank you.

I would just observe that I think the system was working. It was a narrow program that the president explained to congressional leaders. He had his top lawyers in the Department of Justice and the White House review its constitutionality, and he was convinced that it was legal. He narrowly constrained it to international calls, not domestic calls, and al Qaeda-connected individuals. And he also did it with the one group that he has concluded was responsible for 9/11, al Qaeda, the group that this Congress has authorized him to have hostilities against, to go to war against -- and they declared war on us even before 9/11. That's the one group, not other groups that might have hostile interests to the United States like Hezbollah or any other Colombian group or terrorist group around the world. That's what he authorized to occur.

So I think he showed respect for the Congress, not a disrespect. And General Gonzales, other groups that may have violent elements within them are not authorized to be surveiled through this terrorist surveillance program, isn't that correct?

ATTY GEN. GONZALES: Senator, under the -- under the present -- under the present terrorist surveillance program, again as I've indicated, what we're talking about today is people -- members or agents of al Qaeda or related -- of al Qaeda or related terrorist organizations is what we're talking about.

And I think General Hayden I believe testified before the Intel Committee that there are professionals out at NSA, and I presume from other branches of the intel community, that provide input as to what does that mean to be sort of related or working with al Qaeda.SEN JUDICIARY/GONZALES/PM PAGE 96 02/06/2002 .STX

SEN. SESSIONS: Well, let me just conclude with this point. I think the system was working in that way. We were conducting a highly classified, important operation that had the ability to prevent other people from being killed, as Ms. Burlingame's brother was killed and several thousand others on 9/11.

I believe that CIA Director Porter Goss recently in his statement that the revealing of this program resulted in severe damage to our intelligence capabilities is important to note. And I would just like to follow up on Senator Cornyn's questions, General Gonzales, and ask you to assure us that you will investigate this matter, and if people are found to have violated the law, that the Department of Justice will prosecute those cases when they reveal this highly secret, highly important program.

ATTY GEN. GONZALES: Senator, of course we are going to investigate it, and we will make the appropriate decisions regarding a subsequent prosecution.

SEN. SESSIONS: Will the appropriate -- will you prosecute if it's appropriate?

ATTY GEN. GONZALES: We will prosecute when it's appropriate. Yes, sir.

SEN. SESSIONS: Thank you.

SEN. SPECTER: Thank you, Senator Sessions.

Senator Biden.

SEN. JOSEPH BIDEN (D-DE): Thank you very much.

General, how has this revelation damaged the program? I'm always confused about that. I mean, it seems to presuppose that these very sophisticated al Qaeda folks didn't think we were intercepting their phone calls. (Chuckles.) I mean, I'm a little confused. How did it damage this?

ATTY GEN. GONZALES: Well, Senator, I would first defer to the experts in the intel committee who were making that statement, first of all. I'm just a lawyer, so when the director of the CIA says this has really damaged our intel capabilities, I would defer to that statement.

I think, based on my experience, it is true you would assume that the enemy is presuming that we are engaged in some kind of surveillance. But if they're not reminded about it all the time, in the newspapers and in stories, they sometimes forget.

SEN. BIDEN: (Laughs.)

ATTY GEN. GONZALES: And you're amazed at some of the communications that exist. And so when you keep sticking it in their face that we've involved in some kind of surveillance, even if it's unclear in these stories, it can't help but make a difference, I think.

SEN. BIDEN: Well, I hope you and my distinguished friend from Alabama are right that they're that stupid and naive because we are much better off if that's the case. I got the impression from the work I've done in this area that they are pretty darn sophisticated. They pretty well know -- it's a little like when we talk about -- when I say you all haven't -- not you personally -- the administration has done very little for rail security. They've done virtually nothing. And people say, oh, my lord, don't tell them. Don't tell them there are vulnerabilities in the rail system; they'll know to use terror. Don't tell them that that tunnel was built in 1860 and has no lighting, no ventilation. I mean, I hope they're that -- I hope they're that stupid.

ATTY GEN. GONZALES: Sir, I think you can be very, very smart and be careless.

SEN. BIDEN: Well, okay. But if that's the extent of the damage, then I hope we focus on some other things, too.

Look, I'd like to submit for the record a letter to the -- it's probably already been done -- to Senator Specter and Leahy from former Secretary Jamie Gorelick. She makes a very basic point. I don't want to debate it at this time. She said the Aldrich Ames case is a physical search. FISA didn't cover physical searches, as my distinguished friend from Alabama knows. At the time they conducted the search, FISA did not cover physical searches.

And then she went on to say, my testimony did not address whether there would be inherent authority to conduct physical searches if FISA were extended to cover physical searches. After FISA was extended to cover physical searches, to my knowledge FISA warrants were sought.

So I mean, let's compare apples and apples and oranges and oranges.

Let me ask a few other basic questions because, for me, you know, I have real doubts about the constitutionality as others have raised here. But why -- you know, I used to have a friend who used to say, you know, you got to know how

to know. You got to know how to know. And we don't know.

Now you're telling me and the rest of us that the director of CIA said he'd been damaged. Well, the former director told us that we were going to be greeted with open arms; you know, that they had weapons of mass destruction. That was honest mistakes. I mean, for me to accept the assertion made by a single person is something I'd consider, but is not dispositive.

Let me ask you this question. Do you know -- and you may not -- do you know how many of these wiretaps and/or e-mail intercepts have resulted in anything?

ATTY GEN. GONZALES: Well --

SEN. BIDEN: Any criminal referral? Any --

ATTY GEN. GONZALES: Without getting into specifics, Senator, I can say that the director of the FBI said this has been a very valuable program. And it has helped -- it has helped identify would- be terrorists here in the United Statesm and it has helped identify individuals providing material support for terrorists.

General Hayden has said this has been a very successful program; that but for this program they would not have discovered certain kinds of information. General Hayden also said that this program has helped protect and prevent -- I think those were his words -- attacks both here and abroad. These are -- these folks who are paid to make these kinds of assessments. I'm not.

SEN. BIDEN: Have we arrested those people? Have we arrested the people we've identified as terrorists in the United States?

ATTY GEN. GONZALES: Sir, when we can use the law enforcement -- our law enforcement tools to go after the bad guys, we do that.

SEN. BIDEN: No, that's not my question, General. You said that -- you cited the assertions made by Defense Department, by General Hayden, by FBI, that this has identified al Qaeda terrorists. Have we arrested them?

ATTY GEN. GONZALES: Senator, I'm not going to -- I'm not going to go into a specific discussion about --

SEN. BIDEN: I'm not asking for specifics, with all due respect.

ATTY GEN. GONZALES: -- in terms of how that information has been used and the results of that information.

SEN. BIDEN: Well, I hope we arrested them if you identified them. I mean, it kind of worries me because you all talk often about how you identify these people, and I've not heard anything about anybody being arrested. I hope they're not just hanging out there like we had these other guys hanging out prior to 9/11. I don't think you'd make that mistake again.

Can I ask you again, how is this material that proves not to suspected al Qaeda terrorists, calls from Abu Dhabi, American citizen in Selma, Alabama. It turns out that when you do the intercept, the person on the other end from Abu Dhabi wasn't a terrorist -- understandable mistake -- and it turns out the person in Selma wasn't talking to a terrorist. What do you do with that conversation that has now been recorded?

ATTY GEN. GONZALES: What I can say, Senator, is that we do have -- there are minimization procedures in place. You and I had this conversation before about the minimization procedures that may exist with respect to this program.

SEN. BIDEN: That may exist?

ATTY GEN. GONZALES: Meaning --

SEN. BIDEN: Either they do or they don't. Do they?

ATTY GEN. GONZALES: There are minimization procedures that do exist with this program, and they -- and they would govern what happens to that -- to that information.

SEN. BIDEN: Does anybody know what they are?

ATTY GEN. GONZALES: Yes, sir, the folks out at NSA who are actually administering this program.

SEN. BIDEN: Have they told anybody in the Congress? Have they told any court?

ATTY GEN. GONZALES: Sir, I do not know that, the answer to that question.

SEN. BIDEN: I guess -- maybe y'all don't have the same problem I have. If in fact there are minimization procedures and they are being adhered to, no problem. If in fact the people being intercepted are al Qaeda folks and they are talking to American citizens, no problem. But how do we know? I mean, doesn't anybody get to look at this ever? Doesn't a court retrospectively get to look at it? Doesn't the -- this -- this -- you know, the royalty within the Senate get to look at it -- you know, this two, four or eight people? I mean, doesn't somebody look at it?

Or you know, the Cold War lasted 40 years. This war is likely to last 40 years. Is this for 40 years we got to sit here and assume that every president is just, yeah, well, we know old Charlie, he's a good man, we're sure he wouldn't do anything wrong. And we know no one in the intelligence community would ever do anything wrong. We have a history of proving that never occurred. And we know no one in the FBI will ever do anything wrong; that's clear, that never occurred.

I mean is, there some place along the line that somebody other than an analyst who we don't know, but we know he's asserted to be an expert at al Qaeda -- is there somebody other than that person who's ever going to know what happened and whether or not there is -- the next president may be less scrupulous. Maybe he or she will be engaged in data mining.

ATTY GEN. GONZALES: Sir, as I indicated in my opening remarks, of course the inspector general at NSA, he has the responsibility to ensure that the activities under this program are done in a way that's consistent with the president's authorization, including the minimization requirements.

as I indicated in my opening remarks, that of course the inspector general at NSA, he has the responsibility to ensure that the activities under this program are done in a way that's consistent with the president's authorization, including the minimization requirements.

SEN. BIDEN: Okay. This reminds me of a Supreme Court hearing. (Chuckles.)

What -- what goes into the president making his decision on reauthorization every 45 days? Does anybody come and say: Mr. President, look, we have done 2,117 wiretaps, or 219; you've had 60 percent of them had some impact, or only 1 percent has an impact, and we think -- I mean, what -- or is it automatic? I mean, what kind of things does the president look at --

ATTY GEN. GONZALES: No, sir --

SEN. BIDEN: -- other than we still have al Qaeda out there?

ATTY GEN. GONZALES: Sir, it's not automatic. As I also indicated in my opening statement, the president receives information from the intelligence community about the threat. The threat is carefully evaluated as to whether

or not we believe al Qaeda continues to be a continuing threat to the United States of America.

SEN. BIDEN: So long as it is, the program -- so that's the criteria, is al Qaeda a threat? Not: Is the program working? But: Is al Qaeda a threat? Is that the criteria?

ATTY GEN. GONZALES: Well of course not. If we don't have a tool, a lawful tool that's effective, why would we use it? We only use a tool if it's effective.

SEN. BIDEN: (Laughs.) Thank you, General.

ATTY GEN. GONZALES: Mr. Chairman? Mr. Chairman, could I ask for a short break?

SEN. SPECTER: Granted.

ATTY GEN. GONZALES: Thank you, Mr. Chairman.

(Recess.)

SEN. SPECTER: (Sounds gavel.) The Judiciary Committee hearing will resume.

We have four more senators who have not completed their next round who are on the premises. So it may be that we can finish today. Other senators have looked toward another round, so let me negotiate that between today and some date in the future to see if it is necessary to ask you to come back, Mr. Attorney General.

And I had thought about limiting the time to five-minute rounds, but we're going to be here at least until about 5:30, so let's go ahead with the full 10 minutes.

And I'll yield at this time to Senator Graham.

SEN. BIDEN: Mr. Chairman, parliamentary inquiry. I do have other questions. I'm not asking they be asked today or even tomorrow. But if we end today, which I think makes a lot of sense -- the general's been very generous and his physical constitution has been required to be pretty strong here today too. Is it likely, if after you survey us after we close down today, that you may very well ask the general back for more questions from us in open session?

SEN. SPECTER: Senator Biden, I'd like to leave that open. Senator Leahy said that he was looking forward to another round, which is where we were when he left.

SEN. BIDEN: Okay.

SEN. SPECTER: I thought we would have a number of senators who wouldn't have finished a second round, so Attorney General Gonzales would have had to have come back for a second round. But it may be that others will have further questions, or it may be that on some of our other hearings we'll have matters we want to take up with the attorney general. And the attorney general has stated to me his flexibility in coming back. So let's -- is that correct, Mr. Attorney General?

ATTY GEN. GONZALES: I try to be as helpful as I can to you, Mr. Chairman.

SEN. SPECTER: I take that as a yes.

SEN. BIDEN: Ten more seconds. And the only reason I ask, I, like you, want to go to the floor and speak on the asbestos bill that's up. And I didn't know whether I should stay here for a third round or --

SEN. SPECTER: Oh, I can answer that. You should stay here! (Laughter.)

SEN. BIDEN: (Chuckling.) I oppose -- I oppose the chairman's position on asbestos! That's a -- I shouldn't have asked that -- I withdraw the question, Mr. Chairman. Thank you.

SEN. SPECTER: I expect to go till 9:00, Senator Biden. (Laughter.)

SEN. BIDEN: (Laughs.)

SEN. SPECTER: You're going to miss very important materials if you leave. (Laughter.)

Senator Graham.

SEN. LINDSEY GRAHAM (R-SC): Oh, thank you, Mr. Chairman.

Mr. Attorney General, we'll see if we can talk a little bit more about that -- this constitutional tension that we -- that is sort of my pet peeve, for lack of a better word.

I would just echo again what Senator DeWine said. Instead of another around at another time, I would love to engage in a collaborative process with the administration to see if we can resolve this tension.

I want to talk to you exclusively about inherent power and your view of it, and the administration's view of it, and share some thoughts about my view of it.

The signing statement issued by the administration on the McCain language prohibiting cruel, inhumane and degrading treatment, are you familiar with the administration's signing statement?

ATTY GEN. GONZALES: I am familiar with it, Senator.

SEN. GRAHAM: What does that mean?

ATTY GEN. GONZALES: The entirety of the statement, Senator?

SEN. GRAHAM: Well, I mean -- I guess to me, I was taken back a bit by saying "notwithstanding." It was sort of an assertion that the president's inherent authority may allow him to ignore the dictates of the statute.SEN JUDICIARY/GONZALES/PM PAGE 107 02/06/2002 .STX

Does it mean that, or did I misunderstand it?

ATTY GEN. GONZALES: I think -- well, of course, it may mean that this president -- first of all, no president can waive constitutional authority of the executive branch.

SEN. GRAHAM: And my question is very simple, but very important: is it the position of the administration that an enactment by Congress prohibiting the cruel, inhumane and degrading treatment of detainees intrudes on the inherent power of the president to conduct the war?

ATTY GEN. GONZALES: Senator, I think -- I don't know whether or not we have done that specific analysis.

SEN. GRAHAM: Can I ask you this question, then?

ATTY GEN. GONZALES: Yes.

SEN. GRAHAM: Is it the opinion of -- your opinion of the administration's position without the force resolution that FISA is unconstitutional in the sense it intrudes on the power of the president to conduct surveillance in a time of war?

ATTY GEN. GONZALES: I think that question has been raised a couple times today. I've indicated that that then puts us into the third part of the Jackson analysis. I've also indicated that these are difficult questions. Very few --

SEN. GRAHAM: And I'll accept that as an honest, sincere answer because they are difficult.

Let's get back to my scenario about the military member who has a detainee under their charge. They get an order from the commander in chief or some higher authority to do certain techniques. The justification is that we need to know about what's going to happen in terms of battlefield developments. We believe this person possesses information, and those techniques are expressly prohibited by prior statue under the authority of the Congress to regulate the military. That is another classic moment of tension. What do we tell that troop? I mean, if they called you as a lawyer, and they said, "I've got the order from my commander" -- maybe even from the president -- "to engage in five things, but I've been told there's a statute that says I can't do that passed by Congress. What should I do?" What would your answer be to that person?

ATTY GEN. GONZALES: I don't know if I could give that person an immediate answer. That's -- I think that's the point that you are making -- to put our military in that kind of position, that's a very difficult question --

SEN. GRAHAM: Thank you for -- that is absolutely the point I've been trying to make for a year and a half. I want to give that troop an answer that we all can live with.

And let me take this just a little bit further. The FISA statute in a time of war is a check and balance. But here's where, I think, I'm your biggest fan -- during a time of war, the administration has the inherent power, in my opinion, to surveil the enemy and to map the battlefield electronically; not just physical, but to electronically map what the enemy's up to by seizing information and putting that puzzle together.

And the administration has not only the right but the duty, in my opinion, to pursue fifth column movements. And let me tell folks who are watching what a fifth column movement is. It is a movement, known to every war, where Americans, citizens, will sympathize with the enemy and collaborate with the enemy. It's happened in every war. And President Roosevelt talked about -- we need to know about fifth column movements.

So to my friends on the other side, I stand by this president's ability, inherent to being commander in chief, to find out about fifth column movements. And I don't think you need a warrant to do that.

But here's my challenge to you, Mr. Attorney General. There will come a point in time where the information leads us to believe that Citizen A may be involved in a fifth column movement. At that point in time, where we will need to know more about Citizen A's activity on the ongoing basis, here's where I part. I think that's where the courts really come in. I would like you and the next attorney general and next president, if you have that serious information that you need to monitor this American citizen's conduct in the future, that they may be part of a fifth column movement to collaborate the enemy -- I want a check and a balance, because -- here's why.

Emotions run high in war, and we've put a lot of people in prison who just looked like the enemy and never did anything wrong, just as loyal American as you or I. But it would be very easy in this war for an American citizen to be called up by the enemy and labeled as something they're not. It would be very easy, in my opinion, if you're a business person dealing in the Mideast who happens to be American citizen, the business deal goes bad, that bad things could happen to you.

And I would just like the administration to entertain the idea of sitting down with Senator DeWine and others to see if we can find a way, at some point in the process of monitoring fifth column movements, to have a check and balance system that not only would strengthen the commander in chief's role; it will give guidance to the people fighting the war; you'll have Congress on board, you'll be stronger in courts; and the winning -- enemy will be weaker.

How does that proposition sit with you?

ATTY GEN. GONZALES: Senator, the president already said that we'd be happy to listen to your ideas.

SEN. GRAHAM: But you do understand my inherent authority argument -- concern with that argument, because taken -- the next president may not be as sensitive to this limited role of the government. Really, Mr. Attorney General, you could use the inherent authority argument of a commander in chief at a time in war -- almost wipe out anything Congress wanted to do.

ATTY GEN. GONZALES: See, I disagree with that, Senator. I really meant it when I said earlier that in --

SEN. GRAHAM: Give me a situation where the Congress could regulate or trump the inherent power argument when it comes to war.

ATTY GEN. GONZALES: I think Congress has -- a powerful check on the commander in chief is through the purse.

SEN. GRAHAM: If the Congress decided to limit treatment or interrogation techniques of a detainee, would the president have to honor that? Is that part of our authority under the Constitution to regulate the military? Do we have the authority to tell the military you will not do the following things? Would that intrude on the inherent power of the president to run the military?

ATTY GEN. GONZALES: (Inaudible) -- the question is whether or not this is an interference of the day-to-day command functions of the commander in chief or does it fall -- does it fall within that clause of Section 8 of Article I, which says that Congress --

SEN. GRAHAM: Do you believe it's lawful for the Congress to tell the military that you cannot physically abuse a prisoner of war?

ATTY GEN. GONZALES: I'm not prepared to say that, Senator. I think that that's -- I mean, I think you can make an argument that that's part of the rule -- the government --

SEN. GRAHAM: Mr. Attorney General, if we can't do that, if we can't, during a time of war, regulate the behavior of our troops, then really we have no power in a time of war. And that's the point here. I think we share power.

ATTY GEN. GONZALES: I agree. I agree that power is shared in time of war.

SEN. GRAHAM: I think we share a purpose of winning the war.

ATTY GEN. GONZALES: No question about that.

SEN. GRAHAM: But we need to get together so the people on the front lines, who are pulled and torn -- if the Bybee memo, Mr. Attorney General, had become the policy, there would have been people subject to court martial. In your good judgment, you repealed that. But I can assure you, Mr. Attorney General, that the Bybee memo's view of how you handle a detainee and what's torture and what's not, if it had been implemented, it would have violated the Uniform Code of Military Justice, and our guys could have gone to jail. And in your good judgment, you repealed that.

I'm asking for you to use that good judgment again and advise our president to come to this Congress and let us sit down and work through these constitutional tensions, because we don't need tension among ourselves, we need unanimity.

Thank you for your service to our country.

ATTY GEN. GONZALES: Thank you, Senator.

SEN. SPECTER: Thank you very much, Senator Graham.

Senator Durbin?

SEN. RICHARD DURBIN (D-IL): Thank you.

Attorney General, you've said that the safeguards for this program, this terrorist surveillance or domestic spying program, include the fact that they are reviewed by career professionals -- I believe you referred to the National Security Agency, perhaps other agencies -- and that there is a 45-day review as to whether you will continue the program. Where did the 45-day review requirement come from?

ATTY GEN. GONZALES: Senator, that really sort of arose by, quite frankly, schedules in terms of having folks be in a position to provide recommendations and advice as to whether the program can continue. There's nothing magical about the 45 days.

SEN. DURBIN: I'm not worried about the magic so much as the -- is there a statute that drives this?

Is there a legal requirement of a 45-day review?

ATTY GEN. GONZALES: We felt that it -- I think it helps us in the Fourth Amendment analysis in terms of, is this a reasonable search -- the fact that it is reviewed periodically -- and I think it's more sort of by happenstance that it really has come out to be approximately every 45 days.

Let me just also mention that when I talked about the review out of NSA, there are monthly meetings, as I understand it, unconnected with this 45-day review in which senior officials involved in this program sit down and evaluate how the program is being operated. That's a process that's totally independent of this 45-day review process.

SEN. DURBIN: Who chooses the professionals that evaluate this program?

ATTY GEN. GONZALES: Senator, I'm led to believe -- I don't know -- I don't know for sure, but I'm led to believe that they are people -- I'm assuming that senior officials at NSA identify people at NSA who have al Qaeda experience, al Qaeda expertise, knowledge about al Qaeda tactics and aims, and therefore, in the best position to evaluate whether or not a person who's on the call is in fact a member or agent of al Qaeda or an affiliated terrorist organization.

SEN. DURBIN: Which gets to my point, this so-called safeguard -- and it has been referred to as a check and balance -- is literally the administration talking to itself. People within the administration meet within their offices and decide about the civil liberties and freedoms of those who are going to be subjected to this surveillance. That is a significant departure from the ordinary checks and balances of our government, is it not, that all of this is being decided within the same executive branch?

ATTY GEN. GONZALES: I don't know if I -- I don't know if I would characterize that way. I think that there is a lot of -- there is intelligence that is collected by the National Security Agency, where they have control over this information. They have internal rules and regulations. They are subject to minimization requirements. Those are classified. Those have been shared, as I understand it, with the intel committee, if you're talking about Executive Order 12333, and so I don't know that it's so unique to this program.

SEN. DURBIN: Well, let me just say, if you want to wiretap as attorney general, you know what you have to do.

ATTY GEN. GONZALES: Yes, sir.

SEN. DURBIN: You have to go to another branch of our government. You have to get a warrant; that's case -- criminal cases --

ATTY GEN. GONZALES: In a criminal case, Title III, that's right. I mean --

SEN. DURBIN: -- terrorist cases, you know that FISA applies. And now, when it comes to these wiretaps or whatever they may be -- this surveillance, whatever it may be -- you don't go to another branch of government. You meet within your own branch of government, and that I think is a significant difference.

Here's what it comes down to. You know, there's a general concern here as to whether or not -- the scope of what we're talking about and what it might be, and I know you're limited in what you can tell us. But I also know that Michael Chertoff, as secretary of Homeland Security, recently said the NSA was -- quote -- "going through literally thousands of phone numbers and trying to sift through an enormous amount of data very quickly." You've assured us that this is not a dragnet, but I think the thing that it continues to come back to is whether innocent Americans, ordinary Americans, are going to have their e-mails and their phone calls combed through.

And you may shake your head and say, "Oh, we would never do that," but, Attorney General, no one's looking over your shoulder. You're not going to anyone as you would with another wiretap request to determine whether or not it's a reasonable request, or goes to far, or in fact is targeted rather than random.

I talked to you about Mr. Flesher (sp), who's sitting out here, who asked the very basic question: Have I been victimized by this program? Have I been the subject of this program? He couldn't get an answer. He's had communications overseas. The fact that he's sitting here today is a suggestion that he's not worried about what the outcome might be, but he is worried about his freedoms and his liberties. There is no one for him to speak to. When he contacts your administration, they say neither confirm nor deny.

So there's no check and balance here. There's nothing to protect his freedom or liberty, or the freedom and liberty of a lot of innocent people who wonder if you're going too far. That, I think, is why many of us are absolutely stunned that this administration won't come to Capitol Hill and ask us, on a bipartisan basis, for help with this FISA act, if in fact it does create a problem. I voted for the Patriot Act. All but one of the senators in the Senate voted for the Patriot Act. It isn't as if we're not ready to cooperate with you. We would feel better about your conduct and the conduct of this administration if there was a law that you followed. We're not asking you to spell out the operational details, but we're asking you to have at least a FISA Court judge, someone from another branch of government, taking a look at what you're doing. There is some assurance under that situation, for 28 years, that there's a check and balance.

Do you understand why the blank check that you've asked for causes so much heartburn?

ATTY GEN. GONZALES: Senator, I do understand concern about a blank check. I don't believe that that is what we have here.

In your comments you've talked about going around the law, going around FISA. That is not the case here. We believe we are acting consistent with the requirements of FISA.

I don't know about the comments that Secretary Chertoff made. General Hayden has been out very publicly talking about what this program is about, and it is not about -- it doesn't sound like it's the kind of program that Secretary Chertoff is talking about. But I would be very interested in studying his remarks.

This is a very narrowly tailored program.

SEN. DURBIN: How do I know that? There's no one, other than your good word today, there's no one that can tell me: I've looked at this program, trust me, Senator, you can tell Mr. Flesher (sp) and your constituents in Illinois not to worry. We're not going to comb through the records of innocent Americans.

There is no one for me to turn to.

ATTY GEN. GONZALES: I don't know if it's proper to ask you a question, Senator, but I'm going to ask you a question.

SEN. DURBIN: Go ahead. (Laughter.)

ATTY GEN. GONZALES: If we were to brief you into the program, how would anyone be assured that you would protect the rights of ordinary citizens? Because we have briefed congressional leaders, and so they know what we're doing and --

SEN. DURBIN: They are sworn to secrecy, are they not?

ATTY GEN. GONZALES: This is a very classified -- highly classified program.

SEN. DURBIN: They were sworn to secrecy.

ATTY GEN. GONZALES: But they also --

SEN. DURBIN: If they found the most egregious violation of civil rights taking place in this program, they are sworn not to say one word about it.

ATTY GEN. GONZALES: Senator, I've got to believe that all of us, we take an oath of office, and if we honestly believe that a crime is being committed, that we would do something about it.

SEN. DURBIN: How would they? I've been on the intelligence committee, and I can tell you that when you're briefed with classified material -- I sat in briefings not far from here just a few feet away and listened to what I thought was very meager evidence about weapons of mass destruction before the invasion of Iraq. Based on that, I voted against it. But I couldn't walk outside that room until it became public much later and say this administration was at war within when it came to this issue.

ATTY GEN. GONZALES: Senator, I think we're letting members of Congress off the hook easily by saying that as they briefed in the secret program, and they believe it's against the law, that they can't do anything about it. I think you have an obligation, quite frankly, when you take that oath of office -- if you believe that conduct is, in fact, unlawful, I think you can do something about it.

SEN. DURBIN: Well, let's talk about one congressman -- congresswoman, in this case, who has spoken out -- Congresswoman Jane Harman. She's been briefed in the program, and she has said publicly, "You can use FISA. You don't need to do what you're doing. You don't need to go through this warrantless process." So from her point of view, I think she's gone as far as she can go. That's it.

ATTY GEN. GONZALES: Senator, I don't think we've ever said that we couldn't use FISA with respect -- in particular cases. But the time it would take to get a FISA application approved would mean that we may lose access to valuable information.

SEN. DURBIN: You won't come before us and tell us how to change the law to overcome that problem. That is what I find absolutely inexplicable.

The last thing I'd like to do, Mr. Chairman, if -- or whoever's now presiding -- we've had several references to Mrs. Burlingame, who is here, and I thank her for joining us today and for her statements to the press. I would also like to acknowledge the presence of Monica Gabrielle and Mindy Kleinberg, who are also in the families of victims of 9/11. They are here today and they've made a statement for the record. I'll read the last sentence and ask that this be part of the record. "Retaining our civil liberties and our cherished democracy in the face of a looming terrorist threat is the only way we will this war on terror." And I ask that this statement be made a part of the record.

SEN. GRAHAM: Without objection.

SEN. CORNYN: Thank you very much. (Laughter.) Thank you very much, Chairman Graham. Thank you, General.

ATTY GEN. GONZALES: Thank you, Senator. (Laughter.)

SEN. CORNYN: Attorney General Gonzales, Chairman Specter had to step out, but he asked me to proceed after Senator Durbin, and I'm happy to do that so we can move on.

If an employee of the National Security Agency has a concern about the legality of what they're being asked to do, is it -- are they authorized to have a press conference or to otherwise leak that information to outside sources?

ATTY GEN. GONZALES: Senator, I think there are laws that prohibit the disclosure of classified information. I think there might be other ways that may be more -- that would certainly be more appropriate --

SEN. CORNYN: Let me suggest one to you. In 1998 Congress passed the Community Whistle-Blower Protection Act -- Intelligence Community Whistle-Blower Protection Act, which provides in part that an employee of the DIA, the National Imagery and Mapping Agency, the National Reconnaissance Office or the National Security Agency, or a contractor of any of those agencies who intends to report to Congress a complaint about the legality of the program -- that they can report that to the inspector general of the Department of Defense or to the leadership of the Intelligence Committees in the United States Congress. Would you consider that to be a more appropriate place for a so-called whistle- blower to report their concerns?

ATTY GEN. GONZALES: Yes, sir, I would.

SEN. CORNYN: Well, at the very least, there would be an opportunity for those officials to evaluate the complaint of this individual. And we wouldn't have -- we wouldn't risk the disclosure of highly classified information or programs that are collecting intelligence.

ATTY GEN. GONZALES: No question about it. The danger or problem of going to the media as an initial matter is that you have some people, I think, whose motivation, I think, can be questioned in terms of why are they doing that. And when they go out and talk to the public about a highly classified program, they harm the national security of this country. I think Congress realized that when they passed the statute that you just described, to try to provide an avenue for those people who legitimately are concerned about, perhaps, wrongdoing, that they have an avenue to pursue to express their grievances and to do so in a way that we don't jeopardize the nation's secrets.

SEN. CORNYN: Let me ask you -- the last area I want to ask you about -- you've endured through a long day, and I know we're trying to wrap up. I've read a lot about the debate on this program and trying to understand why it is the administration believed that it needed to exercise the authority that it was granted by Congress in the authorization for the use of military force and perhaps the president's power, under the Constitution, over and above what FISA would ordinarily provide.

First of all, if the NSA wants to listen to communications between terrorists abroad that are wholly located in some other country, they can do that without a warrant, can they not?

ATTY GEN. GONZALES: Whether or not FISA applies depends on the answer to basically four key questions. Who is the target? Namely -- primarily, we're concerned about whether or not the communication involves a U.S. person. Where is the target? Primarily we're concerned about whether or not the person is in the United States.

Where is the acquisition taking place? And then finally, what are you trying to acquire? Is it wire communication? Is it radio communication? And so the answer as to whether or not FISA would apply with respect to

a particular communication primarily depends upon answering those kinds of questions.

SEN. CORNYN: Thank you for the precise answer. But as a general matter, if the persons are located in a foreign country and they're not American citizens and the communications are taking place within that foreign country, that FISA does not require the issuance of a warrant.

ATTY GEN. GONZALES: As a general matter, if you're talking about non-U.S. persons outside the United States, and certainly if the acquisition is outside the United States, we don't have to worry about FISA.

SEN. CORNYN: Isn't it true that the problem that this program has tried to address -- the gap in FISA that it tries to address -- is that in order to get a warrant under FISA, the government must have grounds to believe the U.S. person it wishes to monitor is a foreign spy or terrorist? And even if a person is here on a student or tourist visa or no visa, the government can't get a warrant to find out whether they are a terrorist; they must already have reason to believe that they are one?

ATTY GEN. GONZALES: Well, certainly to obtain an order from the FISA court, the court has to be satisfied that there is probable cause to believe that the target is either a foreign power or an agent of a foreign power, and probable cause to believe that the facility being targeted is actually being used or about to be used by a foreign power or an agent of a foreign power.

SEN. CORNYN: Stated another way --

ATTY GEN. GONZALES: (Laughs.) Okay.

SEN. CORNYN: -- the problem with FISA as written is that surveillance -- is, the surveillance it authorizes is unusable to discover who is a terrorist, as distinct from eavesdropping on known terrorists? Would you agree with that?

ATTY GEN. GONZALES: That would be a different way of putting it, yes, sir.

SEN. CORNYN: You wouldn't -- you would agree with that statement?

ATTY GEN. GONZALES: Yes, sir.

SEN. CORNYN: So the particular program that's been debated here and the authority that the National Security Agency has to conduct it is filling a gap that exists in our intelligence-gathering capabilities. Is that an accurate description?

ATTY GEN. GONZALES: I think we quickly realized after the attacks of 9/11 that the tools that we had traditionally been using were insufficient. And this was the opinion of the intelligence community, and that's why the president authorized this program, is because we did have vulnerabilities into our access to information about the enemy.

SEN. CORNYN: Finally, with regard to exclusivity, there have been some on the committee who have asked whether the statement that Congress has made in the FISA statute that it's the exclusive means to gather foreign intelligence, whether that is necessarily a binding obligation when it comes in conflict, if it does, with the Constitution. And I know you've cited the doctrine of, I guess, constitutional avoidance or -- did I get that right?

ATTY GEN. GONZALES: The canon of constitutional avoidance, yes, sir.

SEN. CORNYN: Thank you.

For example -- I mean, this has more than just hypothetical applications. For example, is a police -- are the law enforcement authorities in this country authorized to shoot down a plane that they believe is carrying illegal drugs or

committing some other crime?

ATTY GEN. GONZALES: Senator, I guess I'd have to think about that, if you were asking me whether or not the military have the authorization to shoot down --

SEN. CORNYN: Well, I'm asking you bout law enforcement authorities other than the military.

ATTY GEN. GONZALES: Well, let me just say that we do not expect our law enforcement officers to be perfect in their judgment when you're talking about the Fourth Amendment and searches. The standard is probable cause. It is a reasonable -- it's the totality of the circumstances. But it's very, very important to remember we're talking about the judgment from the eye of a professional officer. Feb 06, 2006 18:45 ET .EOF

And this is what the courts have said. And that's why in the terrorist surveillance program we have the determination made by someone who is experienced regarding al Qaeda tactics and communications. He's making that decision from the view of like the police officer on the beat in terms of what is reasonable, what satisfies the probable cause standard.

SEN. CORNYN: Well, making this very personal and real, if a plane is heading toward the (capital/Capitol ?), don't you believe that the use of force resolution in Article II of the Constitution authorized the president to have the United States military forces shoot that plane down, if necessary?

ATTY GEN. GONZALES: I believe so, sir. And I, quite frankly, believe that the president had the authority prior to the authorization to use military force. I think even though proponents -- pro-Congress group of scholars who believe very strongly in the power of Congress during a time of war, even they acknowledge that with respect to initiation of hostilities, that only the Congress can declare war, but of course military force can be initiated if the United States has been attacked -- initiated by the president if the United States has already been attacked or if there is an imminent threat to the United States.

And so I think there is strong arguments that would support the notion that the president of the United States, even before the authorization to use military force was passed by Congress, after we had been attacked already, of course, could then use military force to repel an additional attack. And we have to remember, of course, that in the days and weeks following 9/11, there were combat air patrols. So the president was exercising his authority, even before the authorization of the use of military force, to have the military in place to protect us from another attack.

SEN. CORNYN: Thank you.

SEN. SPECTER: Thank you, Senator Cornyn.

Senator Kohl?

SEN. HERB KOHL (D-WI): Thank you very much.

Just a couple of questions, Mr. Attorney General. Can you not tell us how many U.S. citizens have had communications intercepted, listened to or recorded by this program since it started?

ATTY GEN. GONZALES: Senator, I wish I could share more information with you, but that information is classified and I can't disclose that.

SEN. KOHL: How many Americans have had their phone conversations recorded or their e-mails intercepted without a court order? Any idea?

ATTY GEN. GONZALES: Again, Senator, you're asking me about the operations of this program and I really can't get into it.

I've outlined today that this is a very narrowly tailored program that's been authorized by the president of the United States, and we have taken great pains to try to protect the privacy interests of every American. But as the president has said, even if you're an American citizen, if you're talking to a member of al Qaeda, we'd like to know why.

SEN. KOHL: You've talked at length today and over the course of the month -- the past month about how the program has to be authorized every 45 days, and you have lauded that as a strong check and a balance on the potential for abuse. And news reports suggest that one of the authorizations has led to changes in the program. Could you tell us what those changes were?

ATTY GEN. GONZALES: Well, again, Senator, you're asking me about operational details of the program, and I really can't get into operational details.

SEN. KOHL: All right. The New York Times reported that in interviews with current and former law enforcement officials that the flood of NSA tips came -- that came from this program led them to expend considerable resources in following the leads, and diverted some agents from work that they had viewed as more productive. Law enforcement officials interviewed said that the program had uncovered no active plots in the United States. One said that, quote, "The information was so thin, the connections were so remote that they never led to anything," unquote. Another said, quote, "It affected the FBI in the sense that they had to devote so many resources to tracking every single one of these leads, and in my experience, they were all dry leads," unquote.

So is there a concern that this program is not collecting enough worthwhile information? And does this suggest that the net was perhaps too large in that you ensnare too many Americans who are not in fact involved in any terrorist activities?

ATTY GEN. GONZALES: Thank you for that question, Senator.

It has been -- I'm aware of these stories. First of all, it is true that Director Mueller feels very strongly that we cannot afford to not investigate one way or the other or to check out every particular tip. We have an obligation to do that.

I think General Hayden has already indicated publicly that immediately following the attacks of 9/11, he exercised his own independent authorities, which do exist for the NSA, to gather up information, gather up more information that they would normally do -- again, these are under existing authorities -- lawful authorities -- and to share all that information with the FBI.

And so, you had a situation where the NSA was gathering up more information than it normally does and then sharing more of that information with the FBI. It -- we quickly discovered that that was not very efficient because of the fact that it required the FBI to utilize their resources. And so that process -- that procedure stopped.

And so I think the stories that you're referred -- referring to do not relate to the terrorist surveillance program about which I'm testifying today.

SEN. KOHL: I thank you very much, and I thank you, Mr. Chairman.

SEN. SPECTER: Thank you, Senator Kohl.

Senator Brownback.

SEN. BROWNBACK: Mr. Chairman, thank you.

General, interesting line of questioning, and I want to pursue going after a FISA warrant with some specificity with you because I want to understand this process better.

And I think you've covered it in bits and pieces today, and I've been in and out at times, but I want to go into it in some depth.

Although before I do that, I want to note in the New York Post, online edition, February 6th, just really in response to the last question here, a 2004 NBC report graphically illustrated -- and I'm reading from this -- what not having the program cost us four and a half years ago. "In 1999, the NSA began monitoring a known al Qaeda switchboard in Yemen that relayed calls from Osama bin Laden to operatives all over the world. Surveillance picked up the phone number of a `Khalid' in the United States, but the NSA didn't intercept those calls, fearing it would be accused of, quote, `domestic spying.' After 9/11, investigators learned that Khalid was Khalid al-Midhar, then living in San Diego under his own name, one of the hijackers who flew American Airlines Flight 77 into the Pentagon. He made more than a dozen calls to the Yemen house where his brother- in-law lived." NBC News called this -- quote -- one of the missed clues that could have saved 3,000 lives.

It's a very real thing and -- very real thing for us today, and one that, had we been operating it effectively prior to 9/11, could have possibly saved thousands of lives.

Mr. Attorney General, we continue to hear and I certainly appreciate the need for expediency in carrying out electronic surveillance. And you've mentioned that getting a FISA warrant is often a time-consuming procedure. I wonder -- could you go into some specificity for me so I can hear this -- how long that process generally takes. Just to the degree you can without revealing information that's classified, how long does this process take?

ATTY GEN. GONZALES: Well, it varies. What I can say, Senator, is that we have, for a variety of reasons, some applications that have been pending for months, quite frankly. Sometimes that's a result because we can't get -- we can't get sufficient information from the FBI or NSA in order to satisfy the lawyers at the department that in fact we can meet the requirements of the FISA act. Sometimes it's a situation where priorities -- you know, every time -- with each passing day, renewals expire on very important programs, and then we -- so we then have to prepare a renewal package to submit to the FISA court, and that means that other FISA applications that our lawyers have been working on kind of get pushed to the side as they work on more important cases.

So there are a variety of reasons why it takes some time to get a FISA application approved.

If you want me to get into a more down in the weeds discussion, it all began --

SEN. BROWNBACK: I would.

ATTY GEN. GONZALES: Okay.

SEN. BROWNBACK: I'd like to get -- you know, what is it that takes so much time in these FISA applications.

ATTY GEN. GONZALES: Well, of course, we can't begin surveillance just based on a whim by someone, say, at the FBI. There has to be a reason to believe that all of the standards of the FISA statute can be satisfied. And we have to know that a FISA Court judge is going to be absolutely convinced that this is an agent of a foreign power; that this facility is going to be a facility that's going to be used or is being used by an agent of a foreign power. The things that I have to approve, I have to -- when I sign an application, I have to -- we have to identify the target, we have to set forth the circumstances and the reasons that I believe that the target is of a foreign power or an agent of a foreign power. I have to set forth the circumstances for why I believe that this facility is being used or about to be used by a foreign power or agent of a foreign power. We have to set forth in the application the minimization requirements that we intend to use. We have to set forth in the application with specificity the type of information we're hoping to get and the type of facilities or communications that we're targeting.

And so those are just some of the things that I have to include in the application. The application has to be accompanied by a certification that is signed by a senior official of the administration who has national security

responsibility. It could be -- normally it's the FBI director. It could be the director of the CIA. And so that person has to certify that in fact this is foreign intelligence information. That person has to certify that the primary purpose -- a significant purpose of the surveillance is for foreign intelligence purposes. That person has to certify that normal investigative techniques or means are not otherwise available. And I think there -- and there are some other provisions that have to be certified.

And so all those conditions, requirements, have to be met even before I authorize verbally an emergency authorization. And it takes time. Even in a perfect world, even in an ideal case, it's going to take a period of time.

And I'm not talking about hours. We're normally talking about days, weeks. On the more complicated cases, again, sometimes months.

SEN. BROWNBACK: And this would include even these sort of operations we've read about data mining operations? Would that include those sorts of operations, or are those totally a separate type of field?

ATTY GEN. GONZALES: I'm not here to talk about that. Again, let me just caution everyone that you need to read these stories with caution. There is a lot of mumbling -- I mean, mixing and mangling of activities that are totally unrelated to what the president has authorized under the terrorist surveillance program, and so I'm uncomfortable talking about other kinds of operations that might -- that are unrelated to the terrorist surveillance program.

SEN. BROWNBACK: These would be strictly ones where you are going after a targeted set of individuals that have gone through --

ATTY GEN. GONZALES: Under FISA or --

SEN. BROWNBACK: Yes, that are done do the FISA application.

ATTY GEN. GONZALES: But we have to remember, of course, this is --

SEN. BROWNBACK: Along the lines of what you've just described in some detail. This is the sort of information you are seeking before you're going after anything under FISA.

ATTY GEN. GONZALES: In every case. And of course we always have to remember that we're not just talking about al Qaeda when you're talking about FISA. You're talking about agents of, you know -- of other countries. And it's not limited to only international communications under FISA. It's domestic communications. So we want to get it right, of course. And as I said earlier in a response to another question, the fact that we've had such a high approval rate by the FISA Court isn't an indication that the FISA Court is a rubber stamp. It is more, I think, proof -- proof that we've got a legitimate process. We take this very seriously.

SEN. BROWNBACK: Well, I don't want to drag on questions. You've been here a long period of time.

I just -- I do want to encourage us that as the war on terrorism wears on -- because it's going to wear on for a period of time -- that we do have a check and balance system in place that's workable so that you can get the type of information that you need that we need to protect the country, but at the same time can protect the civil liberties of the nation, and you're doing everything you can in that regard. I just think as we look on forward, this is going to be a key policy factor of how we move forward and sustain support for the war on terrorism over the periods of various administrations and possible length of time that this could well take.

Thank you for being here. Thank you, Chairman.

SEN. SPECTER: Thank you, Senator Brownback.

Mr. Attorney General, you've held up remarkably well for a long day. I have deferred my second round until

everyone else has concluded the second round because as chairman I have to stay, so I thought I'd go last in any event. So it's just you and me.

When we came in today, there was a long line in the hallway waiting to get in, and now only a few people are here, and the senators' bench is pretty well cleared.

I want to come back to the issue as to whether the resolution authorizing the use of force of September 14th gives the president congressional authority to undertake the electronic surveillance. And I said candidly at the outset that I did not think that it did. And let me explore with you the number of questions I have that I'm interested in the administration's response.

Let me start first with the signing statement of President Carter when he signed the Foreign Intelligence Surveillance Act, 1978, on October 25th. He said in part, quote, "The bill requires for the first time a prior judicial warrant for all electronic surveillance for foreign intelligence or counterintelligence purposes in the United States in which communications of U.S. persons might be intercepted."

He clarifies the executive's authority to gather foreign intelligence by electronic surveillance in the United States. It will remove any doubt about the legality of those surveillances which are conducted to protect our country against espionage and international terrorism, so that when you talk about what happened in Washington's time on intercepting messages or unsealing envelopes or what happened in Lincoln's time or what happened in Franklin Delano Roosevelt's time, or when you talk about a number of the circuit court opinions giving broad presidential authority, saying that the gathering of intelligence was his prerogatives without respect to the Fourth Amendment, that's before Congress acted.

Now a signing statement is subjected to -- subject to a number of limitations.

If the president in the signing statement seeks to, well, distinguish his view from what the Congress has passed, I think you're entitled to very little if any weight.

Where the president, as President Carter did, squarely backs what the Congress has done, then you have a concurrence of the Congress and the president. And you really have very forceful, very plain, very strict language in the Foreign Intelligence Surveillance Act.

How do you counter what President Carter has said: that it applies to all U.S. persons and covers all foreign intelligence by electronic surveillance in the United States?

ATTY GEN. GONZALES: Well, of course, Senator, I don't believe that it is possible for any president to waive for future presidents any constitutional authority, any authority given to a president under the Constitution. Feb 06, 2006 18:47 ET .EOF

I haven't read that statement in a while, but I don't think in the statement President Carter says, "I have no inherent authority remaining in this area."

Finally, I would just simply remind the chair -- I think this was mentioned earlier by one of the senators -- his attorney general in hearings in connection with the legislation -- I think it was before the House -- I think it was before the committee of the House -- talked about the fact that this is -- and I'm paraphrasing here -- this in no way takes away from the president's inherent constitutional authority -- this legislation.

And so that's how I would respond to your question.

SEN. SPECTER: Well, Mr. Attorney General, the -- that's not the Jackson test which you've subscribed to, but I'm going to come back to that in just a minute.

In your responses to my question about statutory interpretation -- and we've covered the line that it is disfavored to

have a repeal by implication -- and you have the statute of FISA specific -- no interception -- no electronic -- no interception of electronic communication without a warrant, which is very specific. And then, you have the generalized statement of the September 14th resolution, which at best would be repealed by implication, which is disfavored.

But then, we come across -- on another very important provision of statutory construction, and that is, the one which relates to specific language, takes precedence over more generalized pronouncements. And in your answer, you said, quote, "It is not clear which provision is more specific," closed quote. Well, that is false on its face. If you have the statute saying, "No electronic surveillance without a warrant," there's no doubt that that is more specific than the September 14th resolution, isn't it?

ATTY GEN. GONZALES: Well --

SEN. SPECTER: How could you disagree with those plain words?

ATTY GEN. GONZALES: -- by that answer I only meant to convey, Senator, that the resolution is more specific with respect to al Qaeda, certainly, and of course the FISA statute is not limited only to al Qaeda.

I might also -- as my -- as the answer also indicates, we had sort of the same -- this same discussion or -- occurred with respect -- in the Hamdi decision. We had the same situation, you had a specific statute, 18 USC 4,0001 (a), that said no American citizen could be detained, except as otherwise provided by Congress or maybe -- otherwise provided by an act of -- a statute by Congress.

And the Supreme Court said that nonetheless, you had a broader authorization in the authorization to use military force and that would satisfy the statute, even though you had a specific statute with respect to detention and you had a broad authorization --

SEN. SPECTER: Did the Supreme Court deal with that statute?

ATTY GEN. GONZALES: The 4001(a)? That was the statute at issue, yes, sir, in the Hamdi decision. Of course.

SEN. SPECTER: Did the Supreme Court deal with it specifically?

ATTY GEN. GONZALES: Sir, in Hamdi, Mr. Hamdi was contesting that that statute prohibited the president of the United States from detaining him because he was an American citizen. And the Supreme Court said, well, okay, you're right, you have this specific statute. But you've also got this broad grant of authority by the Congress and that is sufficient to allow the president of the United States to detain you as an American -- even as an American citizen.

SEN. SPECTER: Well, I think you're dealing with very different circumstances when you talk about a soldier on the field as opposed to a United States person whose conversations are being electronically surveilled.

But let me -- let me move on here. It may well be that you and I won't agree on this point.

The resolution of September 14th did not add the words "in the United States" after the words, quote, "appropriate force." That was rejected to give the president broad authority not just overseas, but in the United States. Isn't that a clear indication of congressional intent not to give the president authority for interceptions in the United States?

ATTY GEN. GONZALES: Sir, I don't know where that record is to reflect that that actually happened. I think the CRS, Congressional Research Service, said that in the legislative history -- and I may be wrong -- it's late -- but I believe that they said there's no record to indicate that that ever occurred, quite frankly.

I think -- I think, as I indicated in my opening statement, I think the American public, I think our soldiers, I think our courts, ought to be able to rely upon the plain language passed by the Congress. And there's no question that the resolution talked about the president of the United States protecting Americans both here and abroad. And we have to

put it in context. We were just attacked here in this country from folks within our country communicating within our country. It's hard to imagine, as smart as you are, that you wouldn't provide the United States the authority, the grant of authority to at least deal with a similar kind of threat to the one we just experienced.

SEN. SPECTER: The law involving wiretapping prior to the enactment of the Foreign Intelligence Surveillance Act, had the preceding sentence, quote: "Nothing contained" -- they're referring to the law -- "shall limit the constitutional power of the president to obtain foreign intelligence information deemed essential to the security of the United States."

When the Foreign Intelligence Surveillance Act was passed, that language was stricken. So by all customary standards of statutory interpretation, FISA -- Foreign Intelligence Surveillance Act -- changed that 180 degrees, didn't it?

ATTY GEN. GONZALES: There is no question, if you look at the legislative history and the record, that Congress intended to try to limit whatever president's inherent authority existed. But there's also, from my review of the record, a clear indication that some members of Congress were concerned about the constitutionality of this effort. I think the House Conference Report talks about the fact this is what we're trying to do, it may be the Supreme Court may have a different view of this. And I'm paraphrasing here, but that's a remarkable acknowledgement by a member of Congress that, geez, is what we're doing here really constitutional?

No question about it that certainly Congress intended to cabin the president's authority, but also Congress, when they passed FISA, included Section 109, which is the main criminal provision in FISA, that talks about you can't engage in electronic surveillance under (cover of ?) of law except as otherwise provided by statute.

So I think -- I think we have to apply a fairly possible reading of the statute in that way in order to avoid a very -- in my judgment a tough constitutional question as to whether or not does the Congress have the constitutional authority to to pass a statute that infringes upon the president's inherent authority as commander in chief to engage in electronic surveillance of the enemy during a time of war.

SEN. SPECTER: I don't think you can use the principle of avoiding a tough constitutional conflict by disagreeing with the plain words of the statute.

Attorney General Gonzales, when members of Congress heard about your contention that the resolution authorizing the use of force amended the Foreign Intelligence Surveillance Act, there was general shock.

ATTY GEN. GONZALES: Sir, we've never asserted that FISA's been amended. We've always asserted that our interpretation of FISA, which contemplates another statute, and we have that here in the authorization to use force, that those complement each other. This is not a situation where FISA has been overridden or FISA has been amended. That's never been our position.

SEN. SPECTER: Well, that just defies logic on plain English. FISA says squarely that you can't have electronic surveillance in the -- of any person without a warrant. And you are saying when you tag onto the -- as other statute, which is in the penal provision, that those words in FISA are no longer applicable, that there's been a later statutory resolution by Congress which changes that.

Attorney General Gonzales, I think we come back to the Jackson formula. And my judgment, with some experience in the field -- and I was starting to tell you how shocked people were when we found out that you thought what we had done on the resolution of September 14th authorized electronic surveillance -- just nobody had that in the remotest concept.

And Senator Graham has articulated in very forceful terms the consequence of the administration making this interpretation; that before you ever get any authority from Congress again, we're going to go through every conceivable

exception we can think of, or we just may not give the authority, because you come back to relying on herent (sic) authority.

And you may have the inherent authority. You may have the Article II authority. But I do not think that any fair, realistic reading of the September 14th resolution gives you the power to conduct electronic surveillance.

And that brings me to really what Jackson said. And it's so wise, it's worth reading again. Quote, "When the president takes measures incompatible with the express or implied will of Congress, his power is at its lowest ebb, for then he can rely only upon his own constitutional powers minus any constitutional powers of Congress over the matter."

Now my reading of this situation legally is that there has been an express will of Congress to the contrary and that when the president seeks to rely upon his own inherent power, then he is disregarding congressional constitutional power.

And then Jackson goes on, quote: "Courts can sustain exclusive presidential control in such a case only by disabling the Congress from acting upon the subject." And I think that's what you're doing. You're disabling Congress from acting on the subject which Congress did, signed by the president.

And then Justice Jackson goes on for the really -- the critical language: "Presidential claim to a power at once so conclusive and preclusive must be scrutinized with caution." That's what we're doing here today. We're going to do it a lot more.

And then these are the critical words, more so than any of the others. Quote, "For what is at stake is the equilibrium established by our constitutional system." And there's a very high value placed on the equilibrium of our constitutional system. That means everything.

ATTY GEN. GONZALES: I agree, Senator.

SEN. SPECTER: Okay. Well, finally we've found something to agree upon.

Now on the issue of the inherent power of the president, I believe the president has very substantial Article II power. I believe he does. And we have to be concerned, as a life-or-death matter, about al Qaeda. We really do. And I subscribe to the good faith of the president as to what he has done here, and I've said that publicly. And I subscribe to your good faith in what you have done here.

And I just hope that there will be oversight somewhere along the line, perhaps in the Intelligence Committee, perhaps in the Intelligence Committee, to get into the details, the interstices, the semicolons, is what you're doing, because I know you can't do that here; but I don't think you can measure the president's inherent authority under Article II without knowing what you're doing, just cannot do it, because that authority is not unlimited. And you've agreed to that.

ATTY GEN. GONZALES: I agree with that.

SEN. SPECTER: It's not a blank check.

ATTY GEN. GONZALES: That is correct, sir.

SEN. SPECTER: So it has to be within the parameters of being reasonable. And the cases, the circuit opinions, emphasize the reasonable parameters. And the Supreme Court hasn't ruled on this issue yet. It's an open question. And the circuit opinions are mostly, if not all, predating the Foreign Intelligence Surveillance Act.

So I just hope the Intelligence Committee is going to come down to brass tacks here, and I hope it's the committee and not just the ranking and chairman. Both Senator Roberts and Senator Rockefeller have expressed forcefully their

concern about not being lawyers and not having an opportunity to present these issues to lawyers to get a legal interpretation to square the facts up with what the law is. They just have been very explicit in their own limitations.

So, in conclusion -- the two most popular words of any presentation -- I hope you will give weighty thought to taking this issue to the Foreign Intelligence Surveillance Court lock, stock and barrel; let them see the whole thing, and let them pass judgment. Because if they disagree with you, it's the equilibrium of our constitutional system which is involved. And the al Qaeda threat is very weighty, but so is the equilibrium of our constitutional system.

ATTY GEN. GONZALES: I agree, Senator.

SEN. SPECTER: And security is very weighty, but so are civil rights.

Thank you very much, Attorney General Gonzales. You have established very forcefully your fortitude and stamina here today, even if we disagree with portions of your case.

ATTY GEN. GONZALES: Thank you, Mr. Chairman.

SEN. SPECTER: That concludes the hearing.

(Sounds gavel.)

LOAD-DATE: February 7, 2006

TAB 14

60 of 71 DOCUMENTS

July, 2002

75 S. Cal. L. Rev. 1083

LENGTH: 45113 words

ARTICLE: DIGITAL DOSSIERS AND THE DISSIPATION OF FOURTH AMENDMENT PRIVACY

NAME: Daniel J. Solove*

BIO: * Assistant Professor, Seton Hall Law School; J.D. Yale, 1997. I would like to thank Rachel Godsil, Ted Janger, Orin Kerr, Raymond Ku, Erik Lillquist, Michael Risinger, Paul Schwartz, Christopher Slobogin, Richard Sobel, Charles Sullivan, Michael Sullivan, Peter Swine and Elliot Turrini.

SUMMARY:
... In the Information Age, an increasing amount of personal information is contained in records maintained by Internet Service Providers (ISPs), phone companies, cable companies, merchants, bookstores, websites, hotels, landlords, employers and private sector entities. ... Protecting privacy with an architecture of power involves erecting a legal structure for responding to the ever-increasing data flows of the Information Age. ... In Part V, I suggest guidelines for an appropriate architecture of power to regulate government access to personal information in third party record systems. ... Since the type of information collection that raises concern involves data gathered from dossiers maintained in private sector entities, I recommend that the architecture should encompass all instances where third parties share personal data contained within a "system of records," a term I borrow from the federal Privacy Act. ... Though somewhat unclear, this privacy policy appears to require a subpoena or court order for the government to obtain personal data. ... Title I applies to wiretapping and bugging. ... In certain respects, Title I's requirements are stricter than those for a Fourth Amendment search warrant. ... A Title I court order requires probable cause and a specific description of where the communication will be intercepted, the type of communication, and the period of time for the interception. ...

TEXT:
[*1084]

I. INTRODUCTION

In the Information Age, an increasing amount of personal information is contained in records maintained by Internet Service Providers (ISPs), phone companies, cable companies, merchants, bookstores, websites, hotels, landlords, employers and private sector entities. Many private sector entities are beginning to aggregate the information in these records to create extensive digital dossiers. n1

The data in these digital dossiers increasingly flows from the private sector to the government, particularly for law enforcement use. Law enforcement agencies have long sought personal information about individuals from various third parties to investigate fraud, white-collar crime, drug trafficking, computer crime, child pornography, and other types of criminal activity. In the aftermath of the terrorist attacks of September 11, 2001, the impetus for the government to gather personal information has greatly increased, since such data can be useful to track down terrorists and to profile airline passengers for more thorough searches. n2 Detailed records of an individual's reading materials, purchases,

diseases, and website activity enable the government to assemble a profile of an individual's finances, health, psychology, beliefs, politics, interests, and lifestyle. n3 This data can unveil a person's anonymous speech and personal associations. n4

The increasing amount of personal information flowing to the government poses significant problems with far-reaching social effects. Inadequately constrained government information-gathering can lead to at least three types of harms. First, it can result in the slow creep toward a totalitarian state. n5 Second, it can chill democratic activities and interfere **[*1085]** with individual self-determination. n6 Third, it can lead to the danger of harms arising in bureaucratic settings. n7 Individuals, especially in times of crisis, are vulnerable to abuse from government misuse of personal information. Once government entities have collected personal information, there are few regulations of how it can be used and how long it can be kept. The bureaucratic nature of modern law enforcement institutions can enable sweeping searches, the misuse of personal data, improper exercises of discretion, unjustified interrogation and arrests, roundups of disfavored individuals, and discriminatory profiling. n8 These types of harms often do not result from malicious intent or the desire for domination. Justice Brandeis was prescient when he observed that people "are naturally alert to repel invasion of their liberty by evil-minded rulers. The greatest dangers to liberty lurk in the insidious encroachment by men of zeal, well-meaning but without understanding." n9

The transfer of personal information from the private sector to the government thus requires some form of regulatory control, a way to balance privacy with effective law enforcement. The first source for protecting privacy against infringement by law enforcement agencies is the Fourth Amendment, which prohibits unreasonable searches and seizures and requires that the government first obtain judicial authorization before conducting a search or seizure. According the Supreme Court, "the overriding function of the Fourth Amendment is to protect personal privacy and dignity against unwarranted intrusion by the State." n10 The Court, however, has held that there is no reasonable expectation of privacy in records maintained by third parties. n11 In the void left by the absence of Fourth Amendment protection, a series of statutes provide some limited **[*1086]** restraints on government access to third party records. n12 The protections of the statutory regime are far less exacting than those of the Fourth Amendment; information can be obtained through mere subpoenas and court orders, which have relatively few constraints and little meaningful judicial oversight. Further, numerous classes of records are not covered at all. Thus, there is a profoundly inadequate legal response to the emerging problem of government access to aggregations of data, "digital dossiers" that are increasingly becoming digital biographies.

A similar scenario unfolded in 1928, when the Supreme Court held in Olmstead v. United States n13 that wiretapping a person's home telephone did not run afoul of the Fourth Amendment. The Court rigidly adhered to a conception of privacy that recognized only physical invasions, which did not include wiretapping because there was no physical trespass to the home. Following Olmstead, Congress enacted 605 of the Federal Communications Act of 1934 to regulate wiretapping, but the law was grossly ineffective. n14 Olmstead left a void in regulating the central threats to privacy in the twentieth century - wiretapping and electronic surveillance - which dramatically increased without adequate regulatory controls and oversight. n15 In 1967, the Court overruled Olmstead. n16 Today, it remains a relic of the past, a long discredited decision. It symbolizes the Court's lack of responsiveness to new technology, unwarranted formalism in its constitutional interpretation, and failure to see the larger purposes of the Fourth Amendment.

Despite the fact that Olmstead was overruled, its spirit has been reincarnated. The new Olmstead era, and its full implications are just beginning to emerge. The Court's current conception of privacy is as a form of total secrecy. n17 As conceived by the Court, an individual's hidden world should be protected. It has expressed an interest in safeguarding the intimate information that individuals carefully conceal. Privacy is about protecting the skeletons that are meticulously hidden in the closet. Since information maintained by third parties is exposed to others, it is not **[*1087]** private, and therefore not protected by the Fourth Amendment. n18 This conception of privacy is not responsive to life in the modern Information Age, where most personal information exists in the record systems of hundreds of entities. The Court has turned its back on one of the most far-reaching and potentially dangerous law enforcement practices of our times. Similar to the 40 years following Olmstead, the only form of regulatory control is statutory, which has thus far has been woefully inadequate.

In this Article, I contend that this state of affairs poses one of the most significant threats to privacy in the twenty-first century. The protection of privacy requires an "architecture of power." n19 This architecture represents the way that law structures social relationships. The law creates and constructs the world we live in by shaping an individual's relationships with other individuals, institutions, and the government. Ideally, the law should establish an architecture of power to maintain an appropriate balance of power in these relationships. Such a balance is critical to dignity, self-fulfillment, freedom, democracy, and other fundamental values. In our highly bureaucratized world, personal information is an essential element of these relationships. Protecting privacy with an architecture of power involves erecting a legal structure for responding to the ever-increasing data flows of the Information Age. Beyond a set of individual rights, protecting privacy requires an architecture that regulates the way information may be collected and used.

The focus of this Article is on our relationships with the government. An architecture of power must address two fundamental problems of government. First, it should address how to control the population without stifling liberty, in other words, how to balance order and freedom. Second, it should determine how to control the government so that it remains accountable to the people. This includes preventing officials from abusing their power, and guarding against excessive growth in government power that threatens to override the power of the people. One of the most **[*1088]** profound powers of the government is its machinery for enforcing the law, which increasingly requires personal information to function. Therefore, an architecture of power must be developed to regulate the flow of personal information between the private sector and the government. In this Article, I compare the architectures established by the Fourth Amendment to the current statutory regulatory regime, and articulate a theory identifying the types of architectural features that will create the appropriate balance between privacy and effective law enforcement.

In Part II, I describe the extensive records of personal information that are maintained by third parties and the rapidly increasing information flows between the government and private sector entities. I illustrate why these information flows present a serious threat to privacy and why an architecture of power is essential to ensure that privacy is adequately protected.

In Part III, I describe the basic architecture of power that the Fourth Amendment endeavors to establish and explain why this architecture has many important features for the effective protection of privacy. Specifically, I contend that the Fourth Amendment embodies a Madisonian theory of government that aims to balance government control with liberty while at the same time keeping government power under control. Substantively, it restricts searches and seizures through the reasonableness requirement and provides procedural safeguards through the warrant and probable cause requirements. These reflect the fractionalization of power among different government branches that James Madison believed was essential to restrain governmental power. I quarrel with a number of prominent critics who contend that the Fourth Amendment should not concern itself with protecting privacy. In the world of modern law enforcement, which has become significantly bureaucratized, privacy is an essential facet of the relationship between the government and the people. I explain at length why this is so, and defend the wisdom of the Fourth Amendment's architecture of power against its critics.

In Part IV, I critique the architecture of power created by the statutory regime that has filled the void left by the inapplicability of the Fourth Amendment to third party records. This architecture of power is a faulty one - uneven, overly complex, filled with gaps and loopholes, and containing numerous weak spots.

In Part V, I suggest guidelines for an appropriate architecture of power to regulate government access to personal information in third party record systems. Regarding the scope of the architecture, I develop a way to define **[*1089]** what types of government information gathering from third parties should be regulated. This is a particularly difficult question. Too broad of a scope could hinder legitimate law enforcement because criminal investigations often require the gathering of data from third parties. Since the type of information collection that raises concern involves data gathered from dossiers maintained in private sector entities, I recommend that the architecture should encompass all instances where third parties share personal data contained within a "system of records," a term I borrow from the federal Privacy Act. Regarding the architecture's structure, I explore a spectrum of procedural mechanisms to establish

the delicate balance between privacy and law enforcement interests. I recommend a fusion of Fourth Amendment architecture and the architecture of subpoenas and court orders.

II. GOVERNMENT INFORMATION GATHERING AND THE PRIVATE SECTOR

A. Third Party Records and the Government

We live in the early stages of the Information Age, a time when technology has given us unprecedented abilities to communicate, transfer and share information, access data, and analyze a profound array of facts and ideas. The complete benefits of the Information Age do not simply come to us. We must "plug in" to join in. In other words, we must establish relationships with a panoply of companies. To connect to the Internet, we must subscribe to an ISP, such as America Online (AOL) or Earthlink. To be able to receive more than a few television channels, we need to open an account with a cable company. Phone service, mobile phone service, and other utilities require us to open accounts with a number of entities.

Further, life in modern society demands that we enter into numerous relationships with professionals (doctors, lawyers, accountants), businesses (restaurants, video rental stores), merchants (bookstores, mail catalog companies), publishing companies (magazines, newspapers), organizations (charities), financial institutions (banks, investment firms, credit card companies), landlords, employers, and other entities (insurance companies, security companies, travel agencies, car rental companies, hotels). Our relationships with all of these entities generate records containing personal information necessary to establish an account and record of our transactions, preferences, purchases, and activities. We are becoming a society of records, and these records are not held by us, but by third parties.

[*1090] In earlier times, communities were smaller and people knew each other's business. Today, the predominant mode of spreading information is not through the flutter of gossiping tongues but through the language of electricity, where information pulses between massive record systems and databases. From the standpoint of individual freedom, this development has both an upside and a downside. Individuals can more readily escape from the curious eyes of the community, freeing themselves from stifling social norms inhibiting individuality and creativity. On the other hand, an ever-growing series of records is created about almost every facet of a person's life.

These record systems are becoming increasingly useful to law enforcement officials. Personal information can help the government detect fraud, espionage, fugitives, smuggling cartels, drug distribution rings, and terrorist cells. Information about a person's financial transactions, purchases, and religious and political beliefs can assist law enforcement in investigating suspected criminals, individuals providing money and assistance to terrorists, or profiling people for more thorough searches at airports. n20

The government, therefore, has compelling reasons to obtain personal information found in records maintained by third parties that can reveal a myriad of details about a person. For instance, from pen registers and trap and trace devices, the government can obtain a list of all the phone numbers dialed to or from a particular location, potentially revealing the people with whom a person associates. From bank records, which contain one's account activity and check writing, the government can discover the various companies and professionals that a person does business with (ISP, telephone company, credit card company, magazine companies, doctors, attorneys, and so on). n21 Credit card company records can reveal where one eats and shops and which cultural events one attends. The government can obtain one's travel destinations and activities from travel agent records. From hotel records, it can discover the numbers a person dialed and the pay-per-view movies a person watched. n22 The government can potentially **[*1091]** obtain one's thumbprint from car rental companies that collect them to investigate fraud. n23 From cable companies, the government can obtain a list of the special pay channels subscribed to or the various pay-per-view events a person has watched. From video stores, the government can access an inventory of the videos that a person has rented.

The government can also glean a wealth of information from the extensive records employers maintain about their employees. n24 Employers frequently monitor their employees. n25 Some use Internet filter software to track how

employees surf the World Wide Web. n26 Employers often keep information about an employee's e-mail use, including back-up copies of the contents of e-mail. A number of employers also conduct drug testing, n27 and many require prospective employees to answer questionnaires asking about drug use, finances, mental health history, marital history, and sexuality. n28 Some even require prospective hires to take a psychological screening test. n29

Landlords are another fertile source of personal information. Landlord records often contain financial, employment, and pet information, in addition to any tenant complaints. Many landlords also maintain logbooks at the front desk where visitors sign in. Some apartment **[*1092]** buildings use biometric identification devices, such as hand scanners, to control access to common areas such as gyms.

Increasingly, companies and entities that we have never established any contact with have dossiers about us. From credit reporting agencies, the government can glean information relating to financial transactions, debts, creditors, and checking accounts. n30 The government can also find out details about people's race, income, opinions, political beliefs, health, lifestyle, and purchasing habits from database companies, since many companies keep extensive personal information on millions of Americans. n31 One database company maintains information about people's supermarket purchases, collected through the use of supermarket discount cards. This data can reveal a complete inventory of one's groceries, over-the-counter medications, hygiene supplies, and contraceptive devices, among others. n32

Beyond the records described above, the Internet has the potential to become one of the government's greatest information gathering tools. n33 There are two significant aspects of the Internet that make it such a revolutionary data collection device. First, it gives many individuals a false sense of privacy. The secrecy and anonymity of the Internet is often a mirage. People are rarely truly anonymous because ISPs keep records of a subscriber's screen name and pseudonyms. n34 ISP account information can also include the subscriber's name, address, phone numbers, passwords, information about web surfing sessions and durations, credit card and bank account information. n35 By learning a person's screen name, the government can identify the person behind the pseudonym postings to newsgroups or chatrooms. For example, in McVeigh v. Cohen, n36 AOL **[*1093]** provided a Navy official with the identity of an individual using a pseudonym who indicated he was gay and worked in the military. Based on this information, the Navy proceeded to initiate discharge proceedings under the "Don't Ask, Don't Tell" policy. n37

A person's ISP can also keep records about websurfing and e-mail activity. At the government's request, an ISP can keep logs of the e-mail addresses with which a person corresponds. Further, the government can use ISP information to find out who uses a particular e-mail address. Thus, it can discover the identities of the individuals with whom a person corresponds. Further, if a person stores e-mail that is sent and received with the ISP, the government can obtain the contents of those e-mails.

Second, the Internet is unprecedented in the degree of detailed information that can be gathered and stored. It is one of the most powerful generators of records in human history. Jerry Kang notes that as we wander through cyberspace, a host of entities assemble information that is "detailed, computer-processable, indexed to the individual, and permanent." n38 For example, as more information goes digital, and as copyright holders seek new ways to profit from their copyrights, the technological tools are in place to monitor the music people listen to and the books people read. n39

Websites often accumulate a great deal of information about their users. Through the use of a "cookie," which identifies a user by deploying a text file into the user's computer, websites can detect the previous website and parts of the site a user accessed. n40 This data is called "clickstream data" because it records nearly every click of the mouse. n41 Another information collection device, known as a "web bug," involves hidden pixel tags secretly planted on a user's hard drive that surreptitiously **[*1094]** gather data about the user. n42 Websites also collect data when people fill out online questionnaires pertaining to their hobbies, health, and interests. Further, a person's Internet postings are archived and do not readily disappear. n43 As we invest more time on the Internet, strangers and unfamiliar organizations are keeping permanent records about our lives.

Thus, the government can glean a substantial amount of information about visitors to a particular website. For

example, certain heath websites ask individuals to fill out questionnaires about their symptoms to determine whether they have a disease. n44 Other websites have questionnaires relating to psychology and personality. n45 From Internet retailers, the government can learn about the books, videos, music, and electronics that one purchases. Some Internet retailers, such as "Amazon.com," record all the purchases a person makes throughout the many years that the person has been shopping on the website. Also, retailers use surveys to identify how a person rates books and videos. n46 Based on this information, the government can discover a consumer's interests, sexuality, political views, religious beliefs, and lifestyle. Further, if a person buys a gift from an Internet retailer and has it mailed to a friend, the government may learn the friend's name and address and develop a list of an individual's friends and acquaintances.

The government may also obtain information from websites that operate personalized home pages. Home pages enable users to keep track of the stocks they own, favorite television channels, airfares for favorite destinations, and news of interest. n47 Other websites, such as Microsoft Network's calendar service, allow users to maintain their daily schedule and appointments. n48 Further, there are some database companies that amass extensive profiles of people's websurfing habits. n49

[*1095] While life in the Information Age has brought us a dizzying amount of information, it has also placed a profound amount of information about our lives in the hands of numerous entities. These digital dossiers are increasingly becoming digital biographies, a horde of aggregated bits of information combined to reveal a portrait of who we are based upon what we buy, the organizations we belong to, how we navigate the Internet, and which shows and videos we watch. n50 This information is not held by trusted friends or family members, but by large bureaucracies that we do not know very well or sometimes do not even know at all.

B. Government-Private Sector Information Flows

Information is becoming more fluid and more readily collected, stored, transferred, and combined with other information. This increasing movement of information is frequently called "information flow." n51 Elsewhere, I have discussed the problems of information flow among various private sector entities n52 as well as from the government to the private sector. n53 There is another problematic type of information flow that is rapidly escalating - data transfers from the private sector to the government.

The government is increasingly contracting with private sector entities to acquire databases of personal information. Database firms are willing to supply the information and the government is willing to pay for it. n54 For example, the private sector company ChoicePoint, Inc. has multimillion dollar contracts with about thirty-five federal agencies including the Federal Bureau of Investigation (FBI) and the Internal Revenue Service (IRS) to provide personal information. n55 ChoicePoint's database contains over ten billion records indexed by Social Security numbers. The information is gathered from public records, private detectives, credit reporting agencies, and other sources. n56

[*1096] The Department of Defense allegedly has purchased information collected by a private sector company about students' web surfing habits. n57 Thus far, the agency has only obtained aggregate information, but in light of the events of September 11, there might be a strong interest in acquiring personally identifiable information about students' web searching habits because some of the terrorists posed as students.

A second form of information flow from the private sector to the government emerges when the government requests private sector records for particular investigations or compels their disclosure by subpoena or court order. Voluntary disclosure of customer information is within the third party company's discretion. n58 Further, whether a person is notified of the request and given the opportunity to challenge it in court is also within the company's discretion. n59

The September 11, 2001 terrorist attacks have changed the climate for private sector-to-government information flows. Law enforcement officials have a greater desire to obtain information that could be helpful in identifying terrorists or their supporters, including information about what people read, with whom they associate, their religion,

and their lifestyle. Following the September 11 attack, the FBI simply has requested records from businesses without a subpoena, warrant, or court order. n60 Recently, Attorney General John Ashcroft has revised longstanding guidelines for FBI surveillance practices. Under the previous version, the FBI could monitor public events and mine the Internet for information only when "facts or circumstances reasonably indicate that a federal crime has been, is being, or will be committed." n61 Under the revised version, the FBI can engage in these types of information gathering without any requirement that this gathering be part of a legitimate investigation or related in any manner to criminal wrongdoing. n62 The FBI can now collect "publicly available information, whether obtained directly or through services or resources (whether nonprofit or commercial) that compile or analyze such **[*1097]** information; and information voluntarily provided by private entities." n63 Further, the FBI can "carry out general topical research, including conducting online searches and accessing online sites and forums." n64

In conjunction with the government's greater desire for personal information, the private sector has become more willing to supply it. Before September 11, the private sector, in certain circumstances, strongly opposed sharing information with the government. For example, when Independent Counsel Kenneth Starr subpoenaed a Washington, D.C. bookstore's records of Monica Lewinsky's purchases, n65 the store spent over $ 100,000 in legal costs vigorously opposing the subpoena. n66 In March of 2000, the Tattered Cover, a bookstore in Denver, Colorado, contested a search warrant in order to protect its customers' privacy. n67 Prior to September 11, an attorney for Amazon.com revealed that law enforcement officials informally requested information about book, music, and video purchases. Amazon.com "typically" informed law enforcement officials that it valued its customers' privacy, it would not disclose their information, albeit with some exceptions. n68

September 11 changed these attitudes. Background check companies, for instance, experienced a large boost in business after September 11. n69 An Internet company shut down its free anonymous Internet surfing **[*1098]** service. n70 Several large financial companies developed agreements to provide information to federal law enforcement agencies. n71

Indeed, in times of crisis or when serious crimes are at issue, the incentives to disclose information to the government are quite significant. Companies do not want to withhold information that will impede the investigation of a terrorist or murderer. They want to cooperate and help out. n72

When private sector entities refuse to cooperate, the government can compel production of the information by issuing a subpoena or obtaining a court order. As discussed in Part IV, these devices are very different from warrants because they offer little protection to the individual being investigated. Notification of the target of the investigation is often within the discretion of the third party. n73 Further, it is up to the third party to challenge the subpoena. n74 So, rather than spend the money and resources to challenge the subpoena, especially when the information is not valuable to their interests, companies can simply turn it over or permit the government to search their records.

Moreover, ISPs are integral to law enforcement officials' ability to investigate. Since September 11, AOL and Earthlink, two of the largest ISPs, have readily cooperated with the investigation of the terrorist attacks. n75 Often, ISPs have their own technology to turn over communications and information about targets of investigations. If they lack the technology, law enforcement officials can install devices such as "Carnivore" to locate the information. n76 Carnivore, now renamed to the more innocuous "DCS1000," is a computer program installed by the FBI at **[*1099]** an ISP. n77 It can monitor all ISP e-mail traffic and search for certain keywords in the content or headers of the e-mail messages. n78

These developments are troubling because private sector companies often have weak policies governing when information may be disclosed to the government. The privacy policy for the MSN network, an affiliation of several Microsoft, Inc. websites such as Hotmail (an e-mail service), Health, Money, Newsletters, eShop, and Calendar, states:

MSN Web sites will disclose your personal information, without notice, only if required to do so by law or in the good

faith belief that such action is necessary to: (a) conform to the edicts of the law or comply with legal process served on Microsoft or the site... . n79

Though somewhat unclear, this privacy policy appears to require a subpoena or court order for the government to obtain personal data.

Amazon.com's privacy policy reads, "We release account and other personal information when we believe release is appropriate to comply with law ... or protect the rights, property, or safety of Amazon.com, our users, or others." n80 It is unclear from this policy the extent to which Amazon.com, in its discretion, can provide information to law enforcement officials.

EBay, a popular online auction website, has a policy stating that

[it] cooperates with law enforcement inquiries, as well as other third parties to enforce laws, such as: intellectual property rights, fraud and other rights. We can (and you authorize us to) disclose any information about you to law enforcement or other government officials as we, in our sole discretion, believe necessary or appropriate, in connection with an investigation of fraud, intellectual property infringements, or other activity that is illegal or may expose us or you to legal liability. n81

This policy gives eBay almost complete discretion to provide the government with whatever information it deems appropriate.

Truste.com, a nonprofit organization providing a "trustmark" for participating websites that agree to abide by certain privacy principles, has drafted a model privacy statement that reads, "We will not sell, share, or **[*1100]** rent [personal] information to others in ways different from what is disclosed in this statement." n82 This policy, however, does not contain any provision about supplying information to the government, and the quoted statement appears to be referring to other private sector entities such as marketers. n83 Further, the policy does not inform people that under existing law, information must be disclosed to the government pursuant to a subpoena or court order. n84

The government is also increasing information flow from the private sector by encouraging it to develop new information-gathering technologies. Private sector firms stand to profit from developing such technologies. Recently, private sector companies have expressed an eagerness to develop national identification systems and face-recognition technology. n85 In addition, the federal government has announced a "wish list" for new surveillance and investigation technologies. n86 Companies that invent such technologies can obtain lucrative government contracts.

The government has also funded private sector information-gathering initiatives. For instance, a company that began assembling a national database of photographs and personal information as a tool to guard against consumer fraud has received $ 1.5 million from the Secret Service to aid in the development of the database. n87

In certain circumstances, where the private sector is not a willing collaborator with the government, new laws require their participation. For example, the Bank Secrecy Act of 1970 requires banks to maintain records of financial transactions to facilitate law enforcement needs, in particular, investigations and prosecutions of criminal, tax, or regulatory matters. n88 Congress passed the Act out of concern that the computerization of records would complicate white-collar crime prosecutions. n89 Under the Act, all federally insured banks must maintain records of each account holder's financial transactions. Furthermore, the Secretary of the Treasury is **[*1101]** authorized to require that certain domestic financial transactions be reported to the government. n90 Under regulations promulgated by the Secretary of the Treasury, a bank must report every financial transaction in excess of $ 10,000. n91

In addition, Congress has passed the Personal Responsibility and Work Opportunity Reconciliation Act of 1996 to

assist with investigations of parents who do not pay child support. It requires that employers collect personal information from all new employees including Social Security numbers, addresses, and wages. n92

Congress has also passed the Communications Assistance for Law Enforcement Act (CALEA) of 1994, n93 which requires telecommunications service providers to develop technology to assist government surveillance of individuals. n94

All of this suggests that businesses and government have become allies. When their interests diverge, new laws requiring cooperation are passed. We are increasingly seeing collusion, partly voluntary, partly coerced, between the private sector and the government.

C. The Dangers of Government Information Gathering

Although there are certainly many legitimate needs for law enforcement officials to obtain personal data, there are also many dangers to unfettered government access to information. There are at least three general types of harms. The first has been discussed under the rubric of the "Big Brother metaphor." n95 Big Brother is the totalitarian government in George Orwell's Nineteen Eighty-Four, which achieved total domination by monitoring every facet of its citizens' private lives. n96 Although elsewhere it is suggested that the Big Brother metaphor does not capture the problem of the collection and use of personal information by private **[*1102]** sector entities, n97 it certainly remains persuasive in the context of government information-gathering. Indeed, historically, totalitarian governments have developed elaborate systems for collecting data about people's private lives. n98 Although the possibility of the rise of a totalitarian state is remote, if our society takes on certain totalitarian features, it could significantly increase the extent to which the government can exercise social control.

Second, government information-gathering can severely constrain democracy and individual self-determination. Paul Schwartz illustrates this with his theory of "constitutive privacy." n99 According to Schwartz, privacy is essential to both individuals and communities: "Constitutive privacy seeks to create boundaries about personal information to help the individual and define terms of life within the community." n100 As a form of regulation of information flow, privacy shapes "the extent to which certain actions or expressions of identity are encouraged or discouraged." n101 Schwartz contends that extensive government oversight over an individual's activities can "corrupt individual decision making about the elements of one's identity." n102 Further, inadequate protection of privacy threatens deliberative democracy by inhibiting people from engaging in democratic activities. n103 This can occur unintentionally; even if government entities are not attempting to engage in social control, their activities can have collateral effects that harm democracy and self-determination.

For example, government information-collection interferes with an individual's freedom of association. The Court has held that there is a "vital relationship between freedom to associate and privacy in one's associations." n104 In a series of cases, the Court has restricted the government's ability to compel disclosure of membership in an organization. n105 In Baird v. State Bar, n106 for example, the Court has declared: "When a State attempts to make inquiries about a person's **[*1103]** beliefs or associations, its power is limited by the First Amendment. Broad and sweeping state inquiries into these protected areas ... discourage citizens from exercising rights protected by the Constitution." n107 The government's extensive ability to glean information about one's associations from third party records without any Fourth Amendment limitations seems to present an end-run around the principles articulated in these cases. n108

Extensive government information-gathering from third party records also implicates the right to speak anonymously. In Talley v. California, n109 the Court struck down a law prohibiting the distribution of anonymous handbills as a violation of the First Amendment. The Court held that "persecuted groups and sects from time to time throughout history have been able to criticize oppressive practices and laws either anonymously or not at all." n110 Further, the Court reasoned, "identification and fear of reprisal might deter perfectly peaceful discussions of public matters of importance." n111 The Court reiterated its view of the importance of protecting anonymous speech in McIntyre v. Ohio Elections Commission. n112 The Court declared that "an author's decision to remain anonymous, like

other decisions concerning omissions or additions to the content of a publication, is an aspect of the freedom of speech protected by the First Amendment." n113 These cases, however, restricted the government from requiring individuals to identify themselves when speaking. With government information-gathering from third parties, namely ISPs, the government can readily obtain an anonymous or pseudonymous speaker's identity. Only computer-savvy users can speak with more secure anonymity. When private parties attempt to obtain the identifying information, courts have held that subpoenas for this information must contain heightened standards. n114 However, no such heightened standards apply when the government seeks to obtain the information.

[*1104] Further, beyond typical anonymity is the ability to receive information anonymously. As Julie Cohen persuasively contends: "The freedom to read anonymously is just as much a part of our tradition, and the choice of reading materials just as expressive of identity, as the decision to use or withhold one's name." n115 The lack of sufficient controls on the government's obtaining the extensive records about how individuals surf the web, the books and magazines they read, and the videos or television channels they listen to can implicate this interest. n116

Additionally, the increasing information flow between the private sector and the government not only implicates the privacy of the target of an investigation, but can also affect the privacy of other individuals. The names, addresses, phone numbers, and a variety of data about a number of individuals can be ensnared in third party records pertaining to the target.

A third type of danger promoted by government information-gathering consists of the harms routinely arising in bureaucratic settings: decisions without adequate accountability, dangerous pockets of unfettered discretion, and choices based on short-term goals without consideration of the long-term consequences or the larger social effects. For example, this can lead to dangers such as hasty judgment in times of crisis, the disparate impact of law enforcement on particular minorities, cover-ups, petty retaliation for criticism, blackmail, framing, sweeping and disruptive investigations, racial, ethnic, or religious profiling, and so on. As David Garrow aptly observes:

I always had been much impressed by Joseph Conrad's message in The Heart of Darkness. I have come to feel, however, that the true nature of evil is much more akin to that described by Hannah Arendt than to **[*1105]** Conrad's horror. The danger we all face is not the consequences of man unbound from the restraints of society. It is the surrender of independent and critical judgment by people who work in large organizations. Evil is far more the product of people in complex institutions acting without personal reflection than it is something inherent in individual man. n117

The most frequent problem is not that law enforcement agencies will be lead by corrupt and abusive leaders, although this arguably happened to some degree for nearly fifty years when J. Edgar Hoover directed the FBI. n118 The problem is the risk that judgment will not be exercised in a careful and thoughtful manner. In other words, it stems from certain forms of government information-gathering shifting power toward a bureaucratic machinery that is poorly regulated and susceptible to abuse. This shift has profound social effects because it alters the balance of power between the government and the people, exposing individuals to a series of harms, increasing their vulnerability and decreasing the degree of power that they exercise over their lives.

As police forces grew in size, number, and technological surveillance capabilities, the relationship between government and citizen transformed. When the Fourth Amendment was ratified, organized police forces did not exist. n119 Colonial policing was "[the] business of amateurs." n120 Sheriffs did not have a professional staff, and relied heavily on ordinary citizens to serve as constables or watchmen, whose primary duties consisted of patrolling rather than investigating. n121 The government typically became involved in criminal investigations only after an arrest was made or a suspect was identified. n122 In ordinary criminal cases, police rarely conducted searches prior to arrest. n123

Organized police forces developed during the nineteenth century, and by the middle of the twentieth century, policing reached an unprecedented level of organization and coordination. n124 At the center of the rise of **[*1106]**

modern law enforcement was the development of the FBI. When the FBI was being formed in 1908, there was significant opposition in Congress to a permanent federal police force. n125 Members of Congress expressed trepidation over the possibility that such an investigatory agency could ascertain "matters of scandal and gossip" that could wind up being used for political purposes. n126 These concerns related to the potential dangers of the agency's information-gathering capabilities, and as will be discussed later, the fears became realities during the course of the FBI's history.

Today, we live in an endless matrix of law and regulation, administered by a multitude of vast government bureaucracies. Like most everything else in modern society, law enforcement has become bureaucratized. n127 There are large police departments armed with sophisticated technology that coordinate with each other. n128 There are massive agencies devoted entirely to investigation and intelligence. As William Stuntz notes, "The problem of discretionary, suspicionless searches and seizures in ordinary criminal cases is an incident of organized police forces - of a system that gives to police officers the job of investigating crimes, identifying suspects, and choosing which suspects to pursue." n129

Many factors make it difficult for law enforcement officials to strike the delicate balance between order and liberty. Among them, there are tremendous pressures on law enforcement agencies to capture criminals, solve notorious crimes, keep crime under control, and prevent acts of violence and terrorism. This highly stressful environment can lead to short cuts, bad exercises of discretion, or obliviousness and insensitivity to people's freedom. One of the most crucial aspects of keeping government power under control is a healthy scrutiny. Most law enforcement officials, however, are unlikely to view themselves with distrust and skepticism. **[*1107]** Police and prosecutors are too enveloped in the tremendous responsibilities and pressures of their jobs to maintain an unbiased and balanced perspective.

In short, one need not fear the rise of a totalitarian state or the inhibition of democratic activities to desire strong controls on the power of the government in collecting personal information. Specifically, government information-gathering must be regulated for a number of reasons.

First, by obtaining private sector records, the government can conduct the type of "fishing expeditions" that the Framers feared. n130 The government can increasingly amass vast dossiers on millions of individuals, conduct sweeping investigations, and search for vast quantities of information from a wide range of sources, without any probable cause or particularized suspicion. Information is easier to obtain, and it is becoming more centralized. Our digital dossiers are beginning to resemble digital biographies that are increasingly flowing to the government. As Justice Douglas noted in his dissent when the Court upheld the constitutionality of the Bank Secrecy Act:

These [bank records] are all tied to one's social security number; and now that we have the data banks, these other items will enrich that storehouse and make it possible for a bureaucrat - by pushing one button - to get in an instant the names of the 190 million Americans who are subversives or potential and likely candidates. n131

Second, as more private sector data becomes available to the government, there could be a de facto national database, or a large database of "suspicious" individuals. n132 Federal governmental entities have conducted substantial information-gathering efforts on political groups throughout the twentieth century. From 1940 through 1973, for example, the FBI and CIA conducted a secret domestic intelligence operation, reading the mail of thousands of citizens. n133 The FBI's investigations extended to members of the women's liberation movement and prominent critics of the Vietnam War, and the FBI obtained information about **[*1108]** personal and sexual relationships that could be used to discredit them. n134 During the McCarthy era and the 1980s, the FBI sought information from libraries about the reading habits of certain individuals. n135 Between 1967 and 1970, the U.S. Army conducted wide-ranging surveillance, amassing extensive personal information about a broad group of individuals. n136 The impetus for the Army's surveillance was a series of riots that followed Dr. Martin Luther King, Jr.'s assassination. n137 The information collected involved data about finances, sexual activity, and health. n138 In 1970, Congress significantly curtailed the

Army's program, and the records of personal information were eventually destroyed. n139 The danger of these information-gathering efforts is not only that it chills speech or threatens lawful protest, but also that it makes people more vulnerable by exposing them to potential future dangers such as leaks, security lapses, and improper arrests. For example, during the late 1960s and early 1970s, the Philadelphia Police Department (PPD) compiled about 18,000 files on various dissident individuals and groups. During a national television broadcast, PPD officials disclosed the names of some of the people on whom files were kept. n140

Third, government entities are using personal information in databases to conduct automated investigations. In 1977, in order to detect fraud, the federal government began matching its computer employee records with those of people receiving federal benefits. n141 With the use of computers to match records of different government entities, the government investigated millions of people. Some matching programs used data obtained from private sector sources (merchants and marketing companies) to discover tax, welfare, and food stamp fraud as well as to identify drug couriers. n142 Computer matching raised significant concerns, and in 1988, **[*1109]** Congress finally passed a law regulating this practice. n143 The law has been strongly criticized as providing scant substantive guidance and having little practical effect. n144 This type of automated investigation is troubling because it alters the way that government investigations typically take place. Usually, the government has some form of particularized suspicion, a factual basis to believe that a particular person may be engaged in illegal conduct. Particularized suspicion keeps the government's profound investigative powers in check preventing widespread surveillance and snooping into the lives and affairs of all citizens. Computer matches, Priscilla Regan contends, investigate everyone, and most people who are investigated are innocent. n145

With the new information supplied by the private sector, there is an increased potential for more automated investigations, such as searches for all people who purchase books about particular topics or those who visit certain websites, or perhaps even people whose personal interests fit a profile for those likely to engage in certain forms of criminal activity. Automated investigations based on profiles share the problems experienced with profiling: the inappropriate use of stereotypes, race, and religion. Profiling or automated investigations based on information gathered through digital dossiers results in targets being inappropriately singled out for more airport searches, police investigations, or even arrest or detention.

Fourth, the government can use dossiers of personal information in mass roundups of distrusted or suspicious individuals whenever the political climate is ripe. As Pamela Samuelson observed: "One factor that enabled the Nazis to efficiently round up, transport, and seize assets of Jews (and others they viewed as "undesirables') was the extensive repositories of personal data available not only from the public sector but **[*1110]** also from private sector sources." n146 In the United States, information gathering greatly assisted the roundups of disfavored groups, including Japanese-Americans during World War II. Following the bombing of Pearl Harbor on December 7, 1941, the FBI detained thousands of Japanese-American community leaders in internment camps. n147 These initial roundups were facilitated by an index of potentially subversive people of Japanese descent compiled by the Justice Department beginning in the late 1930s. n148 In 1942, in the name of national security, about 120,000 people of Japanese descent living on the West Coast were imprisoned in internment camps. n149 The Census Bureau prepared special tabulations of Japanese-Americans, which, according to a 1942 War Department report, "became the basis for the general evacuation and relocation plan." n150

The gathering of personal data also facilitated the Palmer Raids of 1919-20 (also known as the "Red Scare"). In 1991, a rash of bombings sparked the Palmer Raids, one of which damaged the home of Attorney General A. Mitchell Palmer. n151 Bombs went off in eight other cities shortly thereafter and letter bombs were mailed to many elites. n152 In a climate rife with fear of "Reds," anarchists, and labor unrest, n153 Congress tasked the Bureau of Investigation (again, the organization that later became the FBI in 1935) with addressing these terrorist threats. n154 Under the direction of a young J. Edgar Hoover, the Bureau of Investigation developed an extensive index of hundreds of thousands of radicals. n155 This data was used to conduct a massive series of raids, in which over 10,000 individuals suspected of being Communists were rounded up, many without **[*1111]** warrants. n156 The raids resulted in a number of deportations, many based solely on membership in certain organizations. n157 When prominent figures in

the legal community such as Roscoe Pound, Felix Frankfurter, and Zechariah Chafee, Jr., criticized the raids, Hoover began assembling a dossier on each of them. n158

Additionally, personal information gathered by the FBI enabled the extensive hunt for Communists during the late 1940s and 1950s - a period of history that has since been criticized as a severe over-reaction, resulting in the mistreatment of numerous individuals, and impeding the reform agenda begun in the New Deal. n159 According to Ellen Schrecker, federal agencies' "bureaucratic interests, including the desire to present themselves as protecting the community against the threat of internal subversion, inspired them to exaggerate the danger of radicalism." n160 Senator Joseph R. McCarthy, the figure who symbolized the anti-Communist movement, received substantial assistance from Hoover, who secretly released information about suspected Communists to McCarthy. n161 Further, the FBI supplied a steady stream of names of individuals to be called before the House Un-American Activities Committee (HUAC). n162 As Richard Powers observed, "information derived from the [FBI's] files was clearly the lifeblood of the Washington anti-communist establishment." n163 The FBI also leaked information about suspected individuals to employers and the press. n164 Public accusations of being a Communist carried an immense stigma and often resulted in a severe public backlash. n165 Individuals exposed as Communists faced retaliation in the private sector. Numerous journalists, professors and entertainers were fired from their jobs and blacklisted from future employment. n166

[*1112] In short, government entities have demonstrated substantial abilities to gather and store personal information. Combined with the extensive data available about individuals in third party records, this creates a recipe for similar or greater government abuses in the future.

Fifth, unscrupulous government and law enforcement officials can abuse the availability of personal information databases. Recently, a Michigan State Police official allegedly accessed the Law Enforcement Information Network (LEIN), a law enforcement database of personal information, to examine her ex-husband's girlfriend's background. n167 The official was punished with a mere day's suspension without pay. n168 Prior to this incident, allegedly over ninety law enforcement officials had abused the LEIN during the past five years. n169

Sixth, information obtained by the government for one purpose can readily be used for another. For example, the government may be investigating whether a prominent critic of the war against terrorism has in any way assisted terrorists or is engaged in terrorism. In tracking an individual's activities, the government does not discover any criminal activity with regard to terrorism, but discovers that a popular website for downloading music files has been visited and that copyright laws have been violated. n170 Such information may ultimately be used to prosecute copyright violations as a pretext for the government's distaste for the individual's political views and beliefs. Further, dossiers maintained by law enforcement organizations can be selectively leaked to attack critics. n171

Indeed, it is not far-fetched for government officials to amass data for use in silencing or attacking enemies, critics, undesirables, or radicals. For example, J. Edgar Hoover accumulated an extensive collection of files with detailed information about the private lives of numerous prominent individuals, including presidents, members of Congress, Supreme Court **[*1113]** justices, celebrities, civil rights leaders, and attorney generals. n172 Hoover's data often included sexual activities. n173

We live in a world of mixed and changing motives. Data that is obtained for one purpose can be used for an entirely different purpose as motives change. For example, for several years, the FBI extensively wiretapped Martin Luther King, Jr. n174 They wiretapped his home, his office, and the hotel rooms that he stayed at when traveling. n175 Based on the wiretaps, the FBI learned of his extensive partying, extramarital affairs, and other sexual activities. n176 A high level FBI official even anonymously sent him a tape with highlights of the FBI's recordings along with a letter that stated:

King, there is only one thing left for you to do. You know what it is. You have just 34 days in which to do (this exact

number has been selected for a specific reason, it has definite practical significant [sic]). You are done. There is but one way out for you. You better take it before your filthy, abnormal fraudulent self is bared to the nation. n177

Hoover's motive is disputed. One theory is that King was wiretapped because he was friendly with a person who had previously been a member of the Communist Party. n178 Another theory is that Hoover despised King. Hoover's longstanding hatred of King is evidenced by Hoover's nasty public statements about King, such as calling King "the most notorious liar" in the nation. n179 This was probably due, in part, to King's criticism of the FBI for failing to address adequately the violence against blacks in the South, Hoover's overreaction to any criticism of the FBI, and the FBI's practice of consistently targeting its critics. n180 As David Garrow hypothesizes, the original reason that the FBI began gathering information about King was due to fears of Communist ties; however, this motivation **[*1114]** changed once these fears proved unfounded and several powerful individuals at the FBI expressed distaste for King's sexual activities and moral behavior. n181

D. Protecting Privacy with an Architecture of Power

The dangers discussed above illustrate why privacy is integral to freedom in the modern state. Privacy must be protected by establishing an architecture of power. The word "architecture" emphasizes that the protection of privacy must be achieved through establishing a particular social structure that distributes power in our various relationships.

Certain kinds of legal regulation can be readily analogized to architecture. Typically, we view architecture as the design of buildings and edifices. Buildings structure the way people feel and interact; they form and shape human relationships. n182 Neal Kumar Katyal provides a fascinating account of how physical architecture - the way that neighborhoods and buildings are designed - can affect criminal behavior. n183 Law resembles architecture in many respects, especially in the way that certain forms of regulation affect social practices.

If we think of law as creating a structure, we can better understand the different forms that modern regulation must take to protect liberty in the modern state. We have freedom not simply because we have rights. Our liberty is constructed by various regulatory structures that regulate the safety of the products we buy, the conditions of the apartments we live in, the way that companies must interact with us, and the sanctity of the environment, among others. An architecture of power protects a number of social practices of which privacy forms a significant part. It protects **[*1115]** privacy by providing a regulatory structure that shapes relationships and safeguards individual liberties.

At the center of my view is the fact that privacy is an aspect of social practices, which involve relationships with other people and entities. n184 The need for privacy emerges from within a society, from the various social relationships that people form with each other, with private sector institutions, and with the government. We do not need privacy on a deserted island; rather, the need for privacy is engendered by the existence of society, from the fact that we must live together.

Relationships involve some balance of power between the parties. Power is not necessarily a zero-sum good, where more power to one party necessarily means less to another. However, certain configurations of power in these relationships have profound effects on the scope and extent of freedom, democracy, equality, and other important values. In the modern world, we are increasingly finding ourselves in a new type of relationship with public and private institutions. These relationships are different because our institutions are more bureaucratic in nature. Bureaucracies use more information and often exercise power over people through the use of personal data. Collecting and using personal information are having an intensifying influence on the effects of power in our social relationships. Therefore, protecting privacy is critical to governing these relationships, and consequently, to regulating the tone and tenor of life in the Information Age.

Protecting privacy through an architecture of power differs from protecting it as an individual right. Privacy is often viewed as an individual right. n185 It is seen as an individual possession, and its value is defined in terms of its worth to the individual. This view is severely flawed. John Dewey astutely critiqued the "conception of the individual as

something given, complete in itself, and of liberty as a ready-made possession of the **[*1116]** individual, only needing the removal of external restrictions in order to manifest itself." n186 According to Dewey, the individual is inextricably connected to society, n187 and rights are not immutable possessions of individuals, but are instrumental in light of "the contribution they make to the welfare of the community." n188 The problem with viewing rights in purely individualistic terms is that it pits individual rights against the greater good of the community, with the interests of society often winning out because of their paramount importance when measured against one individual's freedom.

Viewing privacy as an individual right against government information-gathering conceives of the harm to privacy as emanating from the invasion into the lives of particular people. But many of the people asserting a right to privacy against government information-gathering are criminals or terrorists, people we do not have a strong desire to protect. In modern Fourth Amendment law, privacy protection is often initiated at the behest of specific individuals, typically those accused of crimes. Often these individuals' rights conflict with the need for effective law enforcement and the protection of society. Why should one individual's preference for privacy trump the social goals of security and safety? This question is difficult to answer if privacy is understood as a right possessed by particular people.

In contrast, an architecture of power protects privacy differently and is based on a different conception of privacy. Privacy is not merely a right possessed by individuals, but is a form of freedom built into the social structure. It is thus an issue about the common good as much as it is about individual rights. It is an issue about social architecture, about the relationships that form the structure of our society.

Government information-gathering is a central facet of our relationships to the government. The increased stores of personal information in the hands of law enforcement officials pose a number of dangers, discussed in the previous section. The abuses of government information-gathering chronicled earlier could be dismissed as those generated by the megalomania of a few rogue officials. David Garrow has another theory, one that is more frightening. According to Garrow, the FBI **[*1117]** that targeted Martin Luther King, Jr. was not a "deviant institution in American society, but actually a most representative and faithful one." n189 In other words, the FBI reflected the mindset of many Americans embodying all the flaws of that mindset. We like to blame individuals, and certainly the particular abusers are worthy of blame, but we cannot overlook the fact that the causes of abuse often run deeper than the corrupt official. Abuse is made possible by a bureaucratic machinery that is readily susceptible to manipulation. Thus, the problem lies in institutional structures and architectures of power. In the latter half of the twentieth century, and continuing to the present, one of the aspects of this architecture has been the lack of control over government information-gathering.

What is the most effective architecture of power to structure the way that the government can access personal information held by third parties? In the pages that follow, I discuss the two relevant architectures, that of the Fourth Amendment, which the Court has concluded does not apply to information held by third parties, and that of the statutory regime that has arisen in the void left by the inapplicability of the Fourth Amendment.

III. THE FOURTH AMENDMENT, RECORDS, AND PRIVACY

A. The Architecture of the Fourth Amendment

1. The Purposes and Structure of the Fourth Amendment

For better or for worse, we currently regulate law enforcement in the United States with a constitutional regulatory regime, comprised primarily by the Fourth, Fifth, and Sixth Amendments. A significant part of this regime applies to government information-gathering. The Fifth Amendment affords individuals a privilege against being compelled to testify about incriminating information. n190 The focus of this Part is the Fourth Amendment, which regulates the ability of the government to obtain information through searches and seizures. The Fourth Amendment provides:

The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath **[*1118]** or affirmation, and particularly describing the place to be searched, and the persons or things to be seized. n191

The Fourth Amendment contains two clauses, the first establishing the right to be secure in persons, houses, papers, and effects against unreasonable searches and seizures and the second stating the requirements for a valid warrant. A long running debate in Fourth Amendment discourse concerns the relationship between the clauses. n192

Substantively, the Fourth Amendment's focus has been on protecting privacy against certain government activities. Procedurally, permissible exercises of government power are controlled through the process of obtaining a warrant supported by probable cause.

The first and most important issue in Fourth Amendment analysis is whether the Fourth Amendment applies to the particular government action. Although the Fourth Amendment applies to government activity in both the civil and criminal contexts, n193 it is limited to activities that constitute "searches" and "seizures." Certain activities, such as seeing things in public, are not searches. n194 Further, the Court has held that the Fourth Amendment only governs searches where an individual has a reasonable expectation of privacy. n195

Once the Fourth Amendment applies, a search or seizure must be "reasonable." n196 Although technically the two clauses of the Fourth Amendment are separate, the Court has interpreted the requirement that a search or seizure be reasonable as closely related to the requirement of a warrant. Generally, searches and seizures without a warrant are per se unreasonable. n197 This has become known as the "per se" warrant rule. n198

Even if the requirements for a valid warrant are established, the Fourth Amendment prohibits the search if it is unreasonable. n199 However, the **[*1119]** Court has rarely found that a search conducted pursuant to a warrant supported by probable cause was unreasonable. n200 Unfortunately, as commentators have pointed out, when the Court has approached what is "reasonable," it has failed to give "reasonable" any teeth. n201 Therefore, if the government obtains a valid search warrant, in most cases the search or seizure is reasonable so long as it is properly within the scope of the warrant.

To obtain a warrant, the police must demonstrate to a neutral judge or magistrate that they have "probable cause" - "where "the facts and circumstances within [the police's] knowledge and of which they had reasonably trustworthy information [are] sufficient in themselves to warrant a man of reasonable caution in the belief that an offense has been or is being committed." n202

Despite the Court's pronouncement in Katz in 1967 that there are only "a few specifically established and well-delineated exceptions" to the warrant requirement, n203 in the decades following Katz, the Court has made numerous exceptions. n204 For example, the Court held in Terry v. Ohio n205 that the police could stop and frisk an individual without a warrant or probable cause. Further, the Court has held that "special needs" in the contexts of schools and workplaces make the warrant and probable cause requirements impracticable. n206 In the words of Silas Wasserstrom and **[*1120]** Louis Michael Seidman, the per se warrant rule "is so riddled with exceptions, complexities, and contradictions that it has become a trap for the unwary." n207

Currently, the Amendment is enforced primarily through the exclusionary rule n208 and, to a lesser degree, through civil liability in 1983 actions. n209 In 1961, in Mapp v. Ohio, n210 the Court held that in all criminal proceedings, both federal and state, evidence obtained in violation of the Fourth Amendment must be excluded from the defendant's criminal trial. n211 According to Arnold Loewy: "The exclusionary rule protects innocent people by eliminating the incentive to search and seize unreasonably." n212 Without the exclusionary rule, Justice Holmes observed, the Fourth Amendment would be a mere "form of words." n213 The exclusionary rule, however, has long been a sore spot in Fourth Amendment jurisprudence, engendering an extensive debate over its desirability and efficacy. n214

[*1121]

2. Fourth Amendment Scope: Privacy

As applied by the Court, the Fourth Amendment has focused on protecting against invasions of privacy, n215 although some commentators contend this focus is misguided. According to William Stuntz, criminal procedure is "firmly anchored in a privacy value that had already proved inconsistent with the modern state." n216 For Stuntz, privacy vis-a-vis the government is impracticable given the rise of the administrative state, with its extensive health and welfare regulation. Stuntz asserts that robust Fourth Amendment protection of privacy will prevent the government from regulating industry, uncovering white-collar crime, and inspecting industry facilities. The government must collect information to enforce certain regulations, such as securities laws, and worker safety protections. n217 "By focusing on privacy," Stuntz argues, "Fourth Amendment law has largely abandoned the due process cases concern with coercion and violence." n218 "The problem," argues Stuntz, "is not information gathering but [police] violence." n219

Scott Sundby offers a different critique of the Fourth Amendment's focus on privacy. Privacy, although "meant to liberate the [Fourth] Amendment from wooden categorizations ... [, has] turned out to contain the seeds for the later contraction of Fourth Amendment rights." n220 "The Fourth Amendment as a privacy-focused doctrine has not fared well with the changing times of an increasingly nonprivate world and a judicial reluctance to expand individual rights." n221 The Fourth Amendment should be redefined as promoting ""trust' between the government and the citizenry." n222 In contrast to totalitarian states, where the government **[*1122]** demonstrates a profound distrust of the people, the government should "trust that the citizenry will exercise its liberties responsibly." n223

However, Sundby assumes that "privacy" means what the Court says it means. Many current problems in Fourth Amendment jurisprudence stem from the Court's failure to conceptualize privacy adequately, both in method and substance. Methodologically, the Court has attempted to adhere to a unified conception of privacy. Conceptualizing privacy by attempting to isolate its essence or common denominator has inhibited the Court from conceptualizing privacy in a way that can adapt to changing technology and social practices. n224 Consider that, substantively, the Court originally conceptualized privacy in physical terms as protecting tangible property or preventing trespasses n225 and that after Katz, the Court shifted to viewing privacy as a form of total secrecy. n226 In each of these conceptual paradigms, the Court has rigidly adhered to a single narrow conception and has lost sight of the Fourth Amendment's larger purposes.

In contrast, the Fourth Amendment provides for an architecture of power, a structure of protection that safeguards a range of different social practices of which privacy forms an integral dimension. Those like Stuntz and Sundby who contend that the Fourth Amendment should not concern itself with privacy fail to see the importance of privacy in the relationship between the government and the people. The private life is a critical point for the exercise of power. Privacy involves aspects of our lives and social practices where people feel vulnerable, uneasy, and fragile. It involves aspects where the norms of social judgment are particularly abrasive and oppressive. It is also implicated where information relates to issues of our most basic needs and desires: finances, employment, entertainment, political activity, sexuality, and family. The private life is an area of profound sensitivity. Control over the private life is one of the central techniques of government power in totalitarian states. Indeed, the great distopian novels of the twentieth century - George Orwell's Nineteen Eighty-Four, Aldous Huxley's Brave New World, and Franz Kafka's The Trial, illustrate how government exercises of power over the private life stifle freedom and well-being. n227

[*1123] Although Stuntz contends that the Fourth Amendment must turn away from privacy after the rise of the administrative state, this is the very reason why it is so important to protect privacy. The rise of the administrative state threatens to give the government excessive power that could destroy the Framer's careful design to ensure that the power of the People remains the strongest. n228 In particular, the extensive power of modern bureaucracies over individuals depends in significant part on the collection and use of personal information. While Stuntz is correct that the Fourth Amendment should not be cabined exclusively to protecting privacy and should address other values, such as coercion and violence, he errs in treating privacy and police coercion as mutually exclusive. n229

Further, robust Fourth Amendment protection need not be inconsistent with the administrative state, as a significant portion of modern administrative regulation concerns business and commercial activities which lack Fourth Amendment rights equivalent to those guaranteed to individuals. n230 Stuntz retorts that for individuals to have a meaningful protection of privacy, they must have privacy within institutions, and giving privacy rights to individuals within institutions "is almost the same as giving the institution itself a protectible privacy interest." n231 Further, Stuntz contends, "a great deal of government information gathering targets individuals," such as the information that is gathered in tax forms. n232 However, one need not adopt an all-or-nothing approach to Fourth Amendment privacy. The Fourth Amendment does not categorically prohibit the government from compelling certain disclosures by individuals or institutions. If it did, then a significant amount of corporate regulation and the tax system would be nearly impossible to carry out. But the fact that the government can compel certain disclosures does not mean that it **[*1124]** can compel people to disclose the details of their sexual lives or require them to send in their diaries and personal papers along with their tax forms. Further, the fact that the government can inspect factories for safety violations and food processing facilities for health violations does not mean that the government should be able to search every employee's office, locker, or bag. Therefore, although misconceptualizing privacy, the Court has correctly made it a focal point of the Fourth Amendment.

3. Fourth Amendment Structure: Warrants

Before eroding it with dozens of exceptions, the Court made the Fourth Amendment's warrant requirement one of the central mechanisms to ensure that the government was exercising its powers of information gathering responsibly. Some critics, however, view warrants as relatively unimportant in the Fourth Amendment scheme, as something to be restricted rather than expanded. According to Akhil Amar, the Fourth Amendment "does not require, presuppose, or even prefer warrants - it limits them. Unless warrants meet certain strict standards, they are per se unreasonable." n233 Amar contends that the colonial revolutionaries viewed warrants with disdain because judges were highly influenced by the Crown and warrants immunized government officials from civil liability after conducting a search. n234 Therefore, according to Amar, "the core of the Fourth Amendment, as we have seen, is neither a warrant nor probable cause, but reasonableness." n235

Amar is too dismissive of warrants. Merely looking to colonial precedents is insufficient, because the Fourth Amendment did not follow colonial precedents (since general searches were rampant) but "repudiated them." n236 My aim, however, is not to quarrel about original intent, as it remains unclear whether the per se warrant rule follows the Framers' intent. Even if Amar is right about the Framers' intent, warrants are an important device in our times since, as Scott Sundby observes, "the Founders could not have foreseen the technological and regulatory reach of government intrusions that exists today." n237

The warrant requirement embodies two important insights of the Framers that particularly hold true today. First, the warrant requirement **[*1125]** aims to prevent searches from turning into "fishing expeditions." n238 Accordingly, the warrant clause circumscribes searches and seizures. A warrant must describe with "particularity ... the place to be searched and the persons or things to be seized." n239

The Framers included the warrant clause because of their experience with general warrants and writs of assistance. n240 The colonists despised writs of assistance because they authorized "sweeping searches and seizures without any evidentiary basis." n241 The Fourth Amendment was inspired by the use of general warrants by Britain, which "resulted in "ransacking' and seizure of the personal papers of political dissenters, authors, and printers of seditious libel." n242 As Patrick Henry declared: "They may, unless the general government be restrained by a bill of rights, or some similar restrictions, go into your cellars and rooms, and search, ransack, and measure, everything you eat, drink, and wear. They ought to be restrained within proper bounds." n243

Second, warrants reflect James Madison's vision of the appropriate architecture of power for a society in which the power of the people remains paramount. Writing about separation of powers in Federalist No. 51, Madison observed:

But what is government itself but the greatest of all reflections on human nature? If men were angels, no government would be necessary. If angels were to govern men, neither external nor internal controuls on government would be necessary. In framing a government which is to be administered by men over men, the great difficulty lies in this: You must first enable the government to controul the governed; and in the next place, oblige it to controul itself. A dependence on the people is no doubt the primary controul on the government; but experience has taught mankind the necessity of auxiliary precautions. n244

[*1126] The profound insight of Madison and the Framers was that by separating government powers between different entities and pitting them against each other, government could be controlled. Madison was acutely aware that the "parchment barriers" of the Constitution would fail to check government encroachments of power, and he explained how both the legislative and executive branches could overstep their bounds. n245 He therefore reasoned that government power should be constrained through governmental architecture, not mere restrictive words. n246 As Madison put it, power should be diffused among different departments of government, each of which should be given "the necessary constitutional means, and personal motives, to resist encroachments of the others," n247 because government will be kept in check only if its parts consist of "opposite and rival interests." n248 Gordon Wood aptly described the Madisonian vision:

It was an imposing conception - a kinetic theory of politics - such a crumbling of political and social interests, such an atomization of authority, such a parceling of power, not only in the governmental institutions but in the extended sphere of the society itself, creating such a multiplicity and a scattering of designs and passions, so many checks, that no combination of parts could hold, no group of evil interests could long cohere. Yet out of the clashing and checking of this diversity, Madison believed the public good, the true perfection of the whole, would somehow arise. n249

The warrant requirement reflects Madison's philosophy of government power by inserting the judicial branch in the middle of the executive branch's investigation process. n250 Although warrants have been criticized as ineffective because judges and magistrates often defer to the police and prosecutor's determination, Christopher Slobogin aptly contends that warrants raise the "standard of care" of law enforcement officials by forcing them to "document their requests for authorization." n251 According to Stuntz, warrants make searching more expensive, because they require law enforcement officials to "draft affidavits and wait around **[*1127]** courthouses." n252 Because officers must devote time to obtaining a warrant, they are unlikely to use them unless they think it is likely that they will find what they are looking for. n253 As Justice Douglas has explained for the Court:

We are not dealing with formalities. The presence of a search warrant serves a high function. Absent some grave emergency, the Fourth Amendment has interposed a magistrate between the citizen and the police. This was done neither to shield criminals nor to make the home a safe haven for illegal activities. It was done so that an objective mind might weigh the need to invade that privacy in order to enforce the law. The right of privacy was deemed too precious to entrust to the discretion of those whose job is the detection of crime and the arrest of criminals. Power is a heady thing; and history shows that the police acting on their own cannot be trusted. And so the Constitution requires a magistrate to pass on the desires of the police before they violate the privacy of the home. n254

Further, the requirement of prior approval prevents government officials from "dreaming up post hoc rationalizations" n255 and from experiencing judicial hindsight bias when evaluating the propriety of a search after it has taken place. n256 As Raymond Ku aptly observes, the Framers adopted the Fourth Amendment based on concerns about limiting executive power. n257

My purpose is not to defend the existing structure of the Fourth Amendment as perfect. For the purposes of this Article, it is sufficient to agree (1) that the Fourth Amendment regime serves an important function by establishing an architecture of power that aims to protect privacy in addition to other values, and (2) that one of the central features of this architecture requires neutral and external oversight of the executive branch's power to gather and use personal information.

[*1128] Even if its efficacy is limited, the structure of the Fourth Amendment is better than a void. Few commentators have suggested that the Fourth Amendment be repealed or that its larger purposes in controlling government power are inimical to a well-functioning society. Outside the realm of the Fourth Amendment is a great wilderness, a jungle of government discretion and uncontrolled power. Thus, the issue of the applicability of the Fourth Amendment is an important one, and to that issue I now turn.

B. The Shifting Paradigms of Fourth Amendment Privacy

Some notion of privacy was always the trigger for Fourth Amendment protection, at least since the late nineteenth century. In 1886, in Boyd v. United States, n258 an early case delineating the meaning of the Fourth and Fifth Amendments, n259 the government attempted to subpoena the records of a merchant for use in a civil forfeiture proceeding. n260 The Court held that the subpoena violated the Fourth and Fifth Amendments:

It is not the breaking of his doors, and the rummaging of his drawers, that constitutes the essence of the offence; but it is the invasion of his indefeasible right of personal security, personal liberty and private property, where that right has never been forfeited by his conviction of some public offence n261

Commentators have characterized Boyd as protecting property and as consistent with the exaltation of property and contract during the Lochner-era. n262 Although Boyd certainly furthers the ideology of the Lochner Court, it should not merely be dismissed as the product of Lochner-like activism. Boyd follows a conception of privacy that the Court consistently adhered to in the late nineteenth century and the first half of the twentieth century. Under this conception, the Court views invasions of privacy as a type of physical injury involving incursions into tangible things.

[*1129] The protection of tangible things extended beyond the home, encompassing the opening of letters sent via the postal system. Nine years prior to Boyd, the Court recognized in 1877, in Ex Parte Jackson, n263 that "the constitutional guaranty of the right of the people to be secure in their papers against unreasonable searches and seizures extends to their papers, thus closed against inspection, wherever they may be." n264 Additionally, privacy also concerned physical bodily intrusions. In Union Pacific Railway Company v. Botsford, n265 an 1891 case concerning privacy but not directly involving the Fourth Amendment, the Court held that a court could not compel a female plaintiff in a civil action to submit to a surgical examination:

The inviolability of the person is as much invaded by a compulsory stripping and exposure as by a blow. To compel any one, and especially a woman, to lay bare the body, or to submit it to the touch of a stranger, without lawful authority, is an indignity, an assault, and a trespass n266

Consistent with Boyd and Ex Parte Jackson, the Court readily recognized the injury caused by physical intrusions such as trespassing into homes, rummaging through one's things, seizing one's papers, opening and examining one's letters, or physically touching one's body. Indeed, in 1890, when Warren and Brandeis authored their famous article The Right to Privacy, they observed that the law, which had long recognized physical and tangible injuries, was just beginning to recognize incorporeal ones. n267 Warren and Brandeis argued that privacy was more than simply a physical intrusion, n268 a view increasingly recognized in the common law of torts in the early twentieth century. n269 However, in its

Fourth Amendment jurisprudence, the Court held fast to its physical intrusion conception of privacy.

The Court's view that Fourth Amendment privacy constituted protection from physical intrusions came to a head in 1928 in Olmstead v. United States. n270 There, the Court held that the tapping of a person's home **[*1130]** telephone outside a person's house did not run afoul of the Fourth Amendment because it did not involve a trespass inside a person's home. More specifically, it held that "the Amendment does not forbid what was done here. There was no searching. There was no seizure. The evidence was secured by the use of the sense of hearing and that only. There was no entry of the houses or offices of the defendants." n271 Olmstead relied upon the Court's physical intrusion conception of privacy. Since there was no trespassing, opening, or rummaging, there was no invasion of Fourth Amendment privacy.

Justice Louis Brandeis vigorously dissented, chastising the Court for failing to adapt the Constitution to new problems. He observed: "When the Fourth and Fifth Amendments were adopted, the form that evil had theretofore taken had been necessarily simple." n272 Furthermore, "[the government] could secure possession of [a person's] papers and other articles incident to his private life - a seizure effected, if need be, by breaking and entry." n273 Brandeis argued that the Fourth Amendment was designed to regulate this conduct - that

"time works changes, brings into existence new conditions and purposes.' Subtler and more far-reaching means of invading privacy have become available to the government. Discovery and invention have made it possible for the government, by means far more effective than stretching upon the rack, to obtain disclosure in court of what is whispered in the closet. n274

The Court, however, followed the Olmstead conception of privacy in Goldman v. United States. n275 The police placed a device called a "detectaphone" on the wall next to a person's office enabling them to eavesdrop on the conversations inside the office. n276 The Court concluded that since there had been no physical trespass into the office, the Fourth Amendment had not been violated. n277

In 1967, nearly forty years after Olmstead, the Court in Katz v. United States n278 finally abandoned the physical intrusion conception of privacy, and adopted the Fourth Amendment approach employed today. Katz involved the wiretapping of a telephone conversation made by the **[*1131]** defendant while in a phone booth. Explicitly overruling Olmstead and Goldman, the Court declared: "What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection. But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected." n279

The Court's approach to determining the applicability of the Fourth Amendment emerged from Justice Harlan's concurrence in Katz. The "reasonable expectation of privacy test" looks to whether (1) a person exhibits an "actual or subjective expectation of privacy" and (2) "the expectation [is] one that society is prepared to recognize as "reasonable."' n280

Brandeis' dissent in Olmstead only partially won the day in Katz. Instead of adopting a conception of privacy that was adaptable to technology, as the new reasonable expectation of privacy test initially had promised to be, the Court rigidified its approach with a particular conception of privacy - total secrecy. The Court centered this new conception on the language in Katz, indicating that privacy turned on what a person exposed to the public. In this way, privacy was conceptualized as a form of secrecy, and one could not have a reasonable expectation of privacy in information that was not kept secret.

The full implications of this new conception of privacy are discussed in the next section. Before turning to this issue, it is important to observe the effects of the Court's failure to conceptualize privacy in Olmstead. As a result of the nearly forty years between Olmstead and Katz, there has been little control over the burgeoning use of electronic

surveillance. Electronic surveillance, one of the most powerful technological law enforcement tools developed during the twentieth century, has profoundly increased the government's powers. The Fourth Amendment, however, has stood by silently as this new technology has developed.

At the time of Olmstead, many viewed wiretapping with great unease. Justice Holmes called it a "dirty business." n281 Even those who became its greatest abusers had initially criticized it. J. Edgar Hoover testified in 1929 that "while it may not be illegal ... [wiretapping] is unethical and it is not **[*1132]** permitted under the regulations by the Attorney General." n282 Hoover stated that "any employee engaged in wire tapping will be dismissed from the service of the bureau." n283

In 1934, just six years after Olmstead, Congress enacted 605 of the Federal Communications Act, making wiretapping a federal crime. However, 605 had significant limitations. It did not apply to wiretapping by state law enforcement officials or by private parties. Nor did it apply to bugging. Further, federal law enforcement officials interpreted 605 merely to preclude the disclosure rather than the collection of intercepted communications. n284 The Supreme Court, however, held that 605 precluded evidence obtained by wiretapping from being used in court. n285 Although law enforcement officials could not use wiretapping evidence or its fruits, 605 failed to prevent them from installing devices and listening. n286

Gradually, presidents gave the FBI increasing authority to wiretap. n287 In World War II, the FBI was authorized to engage in wiretapping to investigate threats to national security. Later, the authorization for wiretapping expanded to encompass domestic security. The fear of communism during the 1950s resulted in further increases in the use of electronic surveillance. n288

As fears of Communism escalated and the authority to engage in electronic surveillance increased, widespread abuses began to occur. Hoover substantially abused his wiretapping authority by extensively wiretapping FBI critics, individuals whose views he disliked, and the enemies of his political allies. n289 As discussed earlier, he engaged in massive electronic surveillance of Martin Luther King, Jr. n290 Presidents also used the wiretapping power of the FBI for their own political purposes and for domestic surveillance. President Nixon ordered extensive wiretapping, including surveillance of his own speechwriter, William **[*1133]** Safire. n291 Presidents Kennedy and Johnson have also been accused of ordering electronic surveillances for improper purposes. n292 With regard to pre-Katz wiretapping by the states, an influential study led by Samuel Dash concluded that 90% of state wiretapping had been done without court authorization and that state regulation of wiretapping had been largely ineffective and impotent against abuses. n293

Thus, for forty years, the government's power to engage in electronic surveillance has fallen outside of the reach of the Fourth Amendment, and the legislation that has filled the void has been ineffective. Today, history is in the process of repeating itself. The Court has made a mistake similar to the one the Olmstead Court made, and it is one with severe and far-reaching implications.

C. The New Olmstead

Although we have moved from the Boyd and Olmstead world of physical papers and places to a new regime based upon expectations of privacy, there is a new Olmstead, one that is just as shortsighted and rigid in approach. The Court's new conception of privacy is one of total secrecy. If any information is exposed to the public or if law enforcement officials can view something from any public vantage point, then the Court has refused to recognize a reasonable expectation of privacy.

For example, in Florida v. Riley, n294 the Court held that a person did not have a reasonable expectation of privacy in his enclosed greenhouse because a few roof panels were missing and the police were able to fly over it with a helicopter. n295 In California v. Greenwood, n296 the police searched plastic garbage bags that the defendant had left on the curb to be collected by the trash collector. The Court held that there was no reasonable expectation of privacy in the trash because "it is common knowledge that plastic bags left on or at the side of a public street are readily accessible

to animals, children, scavengers, snoops, and other members of the public." n297 The Court also reasoned that the trash was left at the curb "for the express purpose of conveying it to a third party, the trash collector, who might **[*1134]** himself have sorted through [the] trash or permitted others, such as the police, to do so." n298

Consistent with this conception of privacy, the Court held that there is no reasonable expectation in privacy for information known or exposed to third parties. In United States v. Miller, n299 federal agents presented subpoenas to two banks to produce all of the financial records of the defendant. The banks produced the records but did not notify the defendant of the subpoenas. The defendant challenged the subpoenas as a violation of the Fourth Amendment. The Court held that there was no reasonable expectation of privacy in financial records maintained by a bank. n300 "The Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities." n301 The Court reasoned: "The checks are not confidential communications but negotiable instruments to be used in commercial transactions. All of the documents obtained, including financial statements and deposit slips, contain only information voluntarily conveyed to the banks and exposed to their employees in the ordinary course of business." n302

In Smith v. Maryland, police officers were attempting to track down a robber who had begun making obscene and harassing phone calls. n303 At one point, the robber asked someone he had been calling to step out on her front porch, where she observed him drive by in his car. n304 The police traced the license plate number and found that the car was registered to the defendant. n305 Without a warrant, the police asked the telephone company to install a pen register to record the numbers dialed from the defendant's home. n306 The Court concluded that there was no reasonable expectation of privacy in pen registers. n307 Since people "know that they must convey numerical information to the phone company" and that the phone company records this information for billing purposes, people cannot "harbor any general expectation that the numbers they dial will remain secret." n308

[*1135] Miller and Smith establish a general rule that if information is in the hands of third parties, then an individual can have no reasonable expectation of privacy in that information, which means that the Fourth Amendment does not apply. n309 Individuals thus probably do not have a reasonable expectation of privacy in communications and records maintained by ISPs or computer network system administrators. n310

Two lines of cases support the third party doctrine. The first deals with standing and the second deals with assumption of risk. The Court's modern standing doctrine emerges primarily from two cases, Rakas v. Illinois n311 and Rawlings v. Kentucky. n312

In Rakas, the police seized evidence from the glove compartment of an automobile with several passengers. The passengers moved to suppress the seized evidence under the Fourth Amendment, but the Court held that they had no standing to do so because they did not own the car and because they claimed that they did not own the evidence in the glove compartment. Said the Court, "[a] person who is aggrieved by an illegal search and seizure only through the introduction of damaging evidence secured by a search of a third person's premises or property has not had any of his Fourth Amendment rights infringed." n313

In Rawlings, a police officer ordered the defendant's girlfriend to empty the contents of her purse. Among the contents of the purse were drugs that the defendant admitted belonged to him. The Court rejected the defendant's Fourth Amendment challenge because he had no reasonable expectation of privacy once he entrusted the items to a third party. n314

In addition to the standing doctrine, both Miller and Smith analogized to a series of cases involving the assumption of risk doctrine. In Miller, the Court noted that "the Fourth Amendment does not "prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed." n315 In Smith, the **[*1136]** Court stated that the defendant had "assumed the risk that the [phone] company would reveal to the police the numbers he [had] dialed." n316

The assumption of risk doctrine emerged from a series of cases dealing with informants and undercover agents. In these cases, either a person had revealed information to a friend, who later divulged the information to the police, or a person revealed the information to a police informant or undercover officer. n317 For example, in Hoffa v. United States, n318 the Court held that the Fourth Amendment did not apply where the defendant made statements to an undercover informant while in his hotel room. n319 The Court reasoned that the undercover informant was "not a surreptitious eavesdropper" but was invited in and trusted by the defendant, who had relied "upon his misplaced confidence that [the informant] would not reveal his wrongdoing." n320 In Lewis v. United States, n321 the defendant sold drugs to an undercover agent, and the Court held that he had assumed the risk of betrayal. n322 Likewise, in Lee v. United States, n323 the Court relied upon the assumption of risk doctrine to reject the claim of a defendant who had revealed information to an informant who was using a concealed transmitter that enabled the police to listen to the conversation. n324

The third party record doctrine, buttressed by the standing and assumption of risk doctrines, stems from a particular conception of privacy that views Fourth Amendment privacy as constituting a form of total secrecy. n325 Under this conception, privacy is a form of concealment, where secrets are inaccessible to others. If information is not secret in this way, if it is in any way exposed to others, then it loses its status as private.

Further, the Court views privacy as an individual right. Fourth Amendment privacy is enforced at the behest of particular individuals via the exclusionary rule. The problem with the Court's current conception of privacy is that it views the Fourth Amendment as protecting rights **[*1137]** possessed by individuals seeking to suppress evidence. According to Mary Coombs, the Court's Fourth Amendment jurisprudence has applied too much of an "individualistic conception of privacy" and has ignored privacy as shared among groups of individuals. n326 Since the Fourth Amendment establishes an architecture of power, its protection should not turn on whether an individual possesses the right. Rather the Amendment protects rights by establishing a particular social structure, one that benefits society by restricting government power. If we most want to protect innocent parties, the Court's standing doctrine thwarts this very goal. n327

Dissenting in Rakas, Justices White, Brennan, Marshall, and Stevens observed that the Court's ruling "undercuts the force of the exclusionary rule in the one area in which its use is most certainly justified - the deterrence of bad-faith violations of the Fourth Amendment." n328 In particular, the Justices observed:

This decision invites police to engage in patently unreasonable searches every time an automobile contains more than one occupant. Should something be found, only the owner of the vehicle, or of the item, will have standing to seek suppression, and the evidence will presumably be usable against the other occupants. n329

Smith and Miller have been extensively criticized throughout the past several decades. However, it is only recently that we are truly beginning to see the profound implications of the Court's third party doctrine. Smith and Miller are the new Olmstead and Goldman. Gathering information from third party records is an emerging law enforcement practice with as many potential dangers as the wiretapping in Olmstead. "The progress of science in furnishing the government with means of espionage is not likely to stop with wiretapping," Justice Brandeis observed in his Olmstead dissent. n330 "Ways may some day be developed by which the government, without removing papers from secret drawers, can reproduce them in court, and by **[*1138]** which it will be enabled to expose to a jury the most intimate occurrences of the home." n331

That day is here. Government information gathering from the extensive dossiers being assembled with modern computer technology poses one of the most significant threats to privacy of our times. In the void left by the inapplicability of the Fourth Amendment, Congress has erected a statutory regime of protection, which establishes the current architecture of power for government information gathering from third party records. Unfortunately, this regime is woefully inadequate.

IV. THE NEW ARCHITECTURE OF POWER: THE EMERGING STATUTORY REGIME AND ITS LIMITS

Throughout the twentieth century, when the Supreme Court held that the Fourth Amendment was inapplicable to new practices or technology, Congress often responded by passing statutes affording some level of protection. Congress through a series of statutes has established a statutory regime regulating government access to third party records. This regime erects a particular architecture of power significantly different from that of the Fourth Amendment. These differences are both substantive (the types of records and information protected) and procedural (the means by which government officials can obtain records). The architecture of this regime is certainly preferable to a void, but is nevertheless substantially inferior to that of the Fourth Amendment. In this Part, I undertake an analysis of this regime, for it is the governing architecture of power for government information-collection from the private sector. Unless the Court reverses course in its Fourth Amendment jurisprudence, it is this regime that must shoulder the burden of balancing order with liberty and keeping government power under control.

A. Statutory Regime Architecture: Scope

1. Wiretapping and Bugging

When the Court held in Olmstead that the Fourth Amendment did not apply to wiretapping, Congress responded six years later by enacting 605 of the Federal Communications Act of 1934. n332 Pursuant to 605, "no person not being authorized by the sender shall intercept any **[*1139]** communication and divulge or publish the existence, contents, substance, purport, effect, or meaning of such intercepted communications to any person." n333 Section 605 did not specify how it was to be enforced, but in Nardone v. United States, the Court held that the exclusionary rule applied in federal court to evidence obtained by wiretapping in violation of 605. n334 However, 605 was a narrow law that did not apply to the states. Consequently, wiretapping by state law enforcement officials was regulated at the state level, and as an influential report concluded, state wiretapping regulation was relatively ineffective. n335 Further, 605 did not cover other means of electronic surveillance such as bugging. Finally, the Department of Justice and the FBI interpreted 605 as only preventing the "divulgence" of information obtained by wiretapping in court, while not prohibiting wiretapping if the information was not used at trial. n336

Section 605 governed wiretapping until United States v. Katz, when the Court finally declared that the Fourth Amendment covered wiretapping. In 1968, Congress enacted the Omnibus Crime Control and Safe Streets Act. n337 Title III of the Act substantially improved the law of wiretapping, extending its reach to state officials as well as to private parties. n338

In 1986, Congress amended Title III with the Electronic Communications Privacy Act (ECPA). The ECPA restructured Title III into three titles: Title I (known as the "Wiretap Act"), dealing with the interception of communications; n339 Title II (known as the "Stored Communications Act"), covering access to stored communications and records; n340 and Title III (known as the "Pen Register Act"), dealing with pen registers and trap and trace devices. n341

Three types of communications are covered by the ECPA. A "wire communication" consists of all "aural" transmissions that travel through a wire, cable, or similar medium. n342 "Aural" means that the transmission must contain a human voice at some point. n343 An "oral communication," is **[*1140]** one that is "uttered by a person exhibiting an expectation that such communication is not subject to interception under circumstances justifying such expectation." n344 Typically, oral communications are those intercepted through bugging devices. n345 Finally, the third type of communication defined by the ECPA is an "electronic communication." Electronic communications are all nonwire and nonoral communications that can be transferred through a wide variety of mechanisms. n346 Typically these consist of text and images (not the human voice) - an e-mail for instance. n347

Title I applies to wiretapping and bugging. A communication must be intercepted in "flight," during transmission. Title I thus somewhat overlaps with the Fourth Amendment because under Katz, the Fourth Amendment applies to

wiretapping. Title I further contains an exclusionary rule, making any unlawfully acquired evidence inadmissible. n348 However, in a significant limitation, the exclusionary rule does not apply to electronic communications. n349 Therefore, the interception of an e-mail is not protected by the exclusionary rule. n350

Title I has strict requirements for obtaining a court order in order to engage in electronic surveillance. n351 In certain respects, Title I's requirements are stricter than those for a Fourth Amendment search warrant. For instance, Title I restricts the type of officials who may apply for a court order and requires that the officials demonstrate that other means for obtaining the information have been unsuccessful. n352 A Title I court order requires probable cause and a specific description of where the communication will be intercepted, the type of communication, and the period of time for the interception. n353 Further, Title I limits the types of crimes that can be investigated with electronic surveillance. For example, a court order cannot be obtained to investigate a misdemeanor. Title I also requires that the court order mandate that the interception be conducted in a **[*1141]** way so as to "minimize the interception of communications not subject to interception." n354

With the exception of electronic communications, which are not protected by an exclusionary rule, Title I has substantial protections. However, they cover ground already safeguarded by the Fourth Amendment. As will be illustrated below, the architecture of the statutory regime is much weaker and more porous in the areas not protected by the Fourth Amendment.

2. Stored Communications

Communications service providers frequently store their customers' communications. These probably fall under the third party-record rule of Smith v. Maryland n355 and United States v. Miller n356 because third parties maintain the information. n357

Although the Fourth Amendment may not protect stored communications, Title II of the ECPA provides some protection. Title II governs stored communications, such as those stored by a phone company or ISP. n358 ISPs temporarily store e-mail communications. For example, suppose Doe sends an e-mail to Roe. The e-mail travels to Roe's ISP and sits there until Roe logs on and downloads her e-mail. Under certain circumstances, a copy of that e-mail may even be kept by Roe's ISP after it is downloaded. With many ISPs, users can also keep copies of previously read e-mail on the ISP's server. Maintaining copies of previously read e-mail with an ISP can be particularly useful, since this enables a person to access the e-mails from remote locations via the Internet. Conversely, if a copy of an e-mail is not kept on the ISP's computer, then it can be accessed only from the particular computer to which it was downloaded. Additionally, ISPs often maintain an outbox folder that contains copies of all the e-mail that a person has sent out.

Title II restricts the government's ability to access communications stored by Roe's ISP. n359 Unfortunately, Title II is quite confusing and its protection is limited. Electronic storage is defined as "any temporary, **[*1142]** intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof," and "any storage of such communication by an electronic communication service for purposes of backup protection." n360 This definition clearly covers e-mail that is waiting on the ISP's server to be downloaded. However, what about e-mail that has been downloaded by the recipient but maintained by the user on the ISP's server? According to the Department of Justice's interpretation of Title II, the copy of the e-mail stored on the server is no longer in temporary storage, and is therefore "simply a remotely stored file." n361 Title II permits law enforcement officials to obtain copies of these communications merely by issuing a subpoena to the ISP. n362

Therefore, the process required for government officials to obtain access to stored communications is considerably less stringent than the Fourth Amendment's warrant requirement. Under Title II, the government must only secure a warrant to obtain the contents of communications in electronic storage for 180 days or less. n363 In the DOJ's view, these communications encompass only unopened e-mail and not previously accessed e-mail stored on an ISP's server. For communications stored over 180 days, the government need only obtain an administrative, grand jury or trial subpoena, or a court order. n364 No probable cause is required. The government must only offer "specific and

articulable facts showing that there are reasonable grounds" to believe communications are "relevant" to the criminal investigation. n365 Recall that Title II does not have an exclusionary rule.

3. Records of Communications Providers

Title II also governs a communications service provider's disclosure of customer records to the government. These provisions differ from the parts of Title II that govern stored communications. Stored communications consist of the traffic of one's correspondence with others, while customer records consist of information about the customer including **[*1143]** name, address, phone numbers, billing records, and types of services the customer has utilized. n366 Recently, the USA-PATRIOT Act has expanded the information that can be obtained from customer records with a subpoena to include "records of session times and durations," "any temporarily assigned network address," and "any credit card or bank account number" used for payment. n367

Under Title II, a communications service provider "shall disclose a record or other information" about a customer when the government obtains a court order. n368 A Title II court order only requires that the government provide "specific and articulable facts showing that there are reasonable grounds to believe that ... the records or other information sought, are relevant and material to an ongoing criminal investigation." n369

One of the most important pieces of information an ISP has in its records is the customer's identity. A customer may use a pseudonym (a screen name), and an ISP may have information linking that pseudonym to the customer's real name. Thus, an ISP often holds the key to one's ability to communicate anonymously on the Internet. The government often wants to obtain this information to identify a particular speaker.

For example, in United States v. Hambrick, n370 a police officer served the defendant's ISP, Mindspring, with a blatantly invalid subpoena that had been "judicially" authorized by another police officer. n371 Although the court recognized that the subpoena was invalid, the evidence was not suppressed due to Title II's lack of an exclusionary remedy. n372

In United States v. Kennedy, an anonymous person called an employee at Road Runner (the defendant's ISP) and informed him that while scanning other computers on the Internet, he had discovered child pornography on the computer of the defendant, who was a Road Runner customer. n373 The caller gave Road Runner the Internet Protocol (IP) address of the defendant's computer. n374 Road Runner then contacted the FBI. n375 The FBI obtained a court order for the defendant's subscriber **[*1144]** information. n376 Eventually this led to the defendant's conviction for possession of child pornography. n377 The court rejected the defendant's Fourth Amendment claim based on the third party doctrine: "When the defendant entered into an agreement with Road Runner for Internet service, he knowingly revealed all information connected to [his] IP address." n378 Instead, Title II applied, and the court concluded had that the court order was defective because the government's application failed to state enough specific facts to meet Title II's requirements. However, the court noted that there was no suppression remedy for such violations. n379

4. Pen Registers, E-mail Headers, and Websurfing

The ECPA also attempts to fill the void left by Smith v. Maryland by addressing pen registers and trap and trace devices. Under Title III of the ECPA, the government must obtain a court order before installing and using a pen register or trap and trace device. n380 However, the court order merely requires that the government demonstrate that "the information likely to be obtained by such installation and use is relevant to an ongoing criminal investigation." n381 In contrast to the Fourth Amendment, probable cause is not required, nor must the target be a criminal suspect. Once the government official makes the proper certification, the court must issue the order. Consequently, courts have little discretion in granting Title III orders. n382 Orders can last up to sixty days. n383 Finally, there is no exclusionary rule for Title III violations.

The USA-PATRIOT Act of 2001 has substantially enlarged the definition of pen registers and trap and trace

devices. Where before a pen register was defined as a device that records "the numbers dialed ... on the telephone line," the new definition encompasses devices and processes that record "dialing, routing, addressing, or signaling information" for a wide variety of transmission facilities beyond telephone lines. n384 A pen register now applies to addressing information on e-mails and to "IP addresses." n385 **[*1145]** An IP address is the unique address assigned to a particular computer connected to the Internet. All computers connected to the Internet have an IP address. All websites also have an IP address. Consequently, a list of IP addresses accessed reveals the various websites that a person has visited. Because websites are often distinctively tailored to particular topics and interests, a comprehensive list of them can reveal a lot about a person's life.

5. Financial Records

Congress has filled the void created by United States v. Miller, which held that bank records are not protected by the Fourth Amendment. The Right to Financial Privacy Act (RFPA) requires that government officials first obtain a warrant or subpoena before accessing financial information. n386 The subpoena merely requires a "reason to believe that the records sought are relevant to a legitimate law enforcement inquiry." n387 The customer must be served with the subpoena prior to its service on the financial institution. Notice, however, can be delayed in a number of circumstances. n388 When information is "relevant to legitimate law enforcement inquiry" and subpoena authority is not available to the government, the government need only submit a formal written request for the information. n389

In addition to banks, credit-reporting agencies have detailed records for nearly every adult American consumer. Under the Fair Credit Reporting Act (FCRA) of 1970, a consumer reporting agency "may furnish identifying information respecting any consumer, limited to his name, address, former addresses, places of employment, or former places of employment, to a governmental agency." n390 Thus, the government can simply request this information without any court involvement. If the government desires to obtain additional information contained in credit reports, it must obtain a court order or grand jury subpoena. n391 The FCRA focuses on consumer reporting agencies. Nothing in the FCRA limits the recipients of credit reports from disclosing them to the government. Credit reports about an individual are frequently supplied to a variety of entities, such as banks, creditors, landlords, and employers.

[*1146] Additionally, the FCRA requires a credit reporting agency to furnish the FBI with a list of all financial institutions where a person maintains an account "when presented with a written request" signed by the FBI director or designee. n392 This provision is limited to foreign counterintelligence investigations and to individuals believed to be foreign agents. n393

Although the RFPA and FCRA protect financial information maintained by banks and credit reporting agencies, the government can obtain financial information from ISPs, employers, landlords, merchants, creditors, and database companies, among others. Therefore, financial records are protected based only on which entities possess them. Thus, the statutory regime merely provides partial protection of financial data.

6. Electronic Media Entertainment Records

The statutory regime protects records pertaining to certain forms of electronic media entertainment. Cable records are afforded a substantial amount of protection. Cable service providers maintain records about their customers, including the fee-based channels, such as HBO, to which the customer subscribes along with the pay-per-view movies a customer orders. Under the Cable Communications Policy Act (Cable Act) of 1984, n394 a government official must obtain a court order in order to obtain cable records. The government must offer "clear and convincing evidence that the subject of the information is reasonably suspected of engaging in criminal activity and that the information sought would be material evidence in the case." n395 Further, the subject of the information can "appear and contest" the court order. n396 This standard is more stringent than the Fourth Amendment's probable cause and warrant requirements. However, there is no exclusionary rule under the Cable Act. The USA-PATRIOT Act has limited the Cable Act by providing that it does not apply to cable Internet service. n397 Thus, where a cable service provider acts as an ISP, the ECPA governs, not the Cable Act.

In addition to cable records, the statutory regime also protects video tape rental records. The Video Privacy Protection Act (VPPA) of 1988, n398 which was passed after reporters hadobtained Supreme Court Justice **[*1147]** Nominee Robert Bork's video cassette rental records, states that a video tape service provider may disclose customer records to law enforcement officials "pursuant to a warrant ... , an equivalent State warrant, a grand jury subpoena, or a court order." n399 Therefore, unlike the Cable Act, the level of protection under the VPPA is much less stringent.

Although the statutory regime protects the records of certain forms of electronic media entertainment, it fails to protect the records of many others. For example, records from music stores, electronics merchants, and Internet media entities are afforded no protection.

7. Medical Records

The recently promulgated federal health privacy rules, pursuant to the Health Insurance Portability and Accountability Act (HIPAA) of 1996, n400 permit law enforcement officials to access medical records with a warrant, court order, or subpoena. n401 Health information may also be disclosed "in response to a law enforcement official's request for such information for the purpose of identifying or locating a suspect, fugitive, material witness, or missing person." n402 Similar to the statutes governing other records, health information can be obtained with a mere subpoena.

Not all health records, however, are covered by HIPAA. Only records maintained by health plans, health care clearinghouses, and health care providers are covered. n403 Doctors, hospitals, pharmacists, health insurers, and Health Maintenance Organizations (HMOs) are covered, but third parties that may have medical information are not covered. Only organizations that engage in "standard transactions" under HIPAA's administrative simplification process for health insurance claims fall within the protections of the regulations. n404 For example, the sale of nonprescription drugs and the rendering of medical advice by many Internet health websites are not covered by HIPAA. n405 As a recent report about the limits of HIPAA has concluded:

Many Web sites offer a "health assessment" feature where users may enter all sorts of information from height and weight to drug and alcohol **[*1148]** use... . For example, HealthStatus.com offers free general health assessments as well as disease specific assessments to determine an individual's risk for some of the leading causes of death... . Because HealthStatus.com does not accept any insurance it will not be covered by the privacy rule... . n406

Therefore, while certain health records are protected, many are not.

8. Holes in the Regime

Federal statutes provide some coverage of the void left by the inapplicability of the Fourth Amendment to records held by third parties. Although they apply to various types of information, such as communication records, financial records, entertainment records, and health records, these records are only protected when in the hands of certain third parties. Thus, the statutory regime does not protect records based on the type of information contained in the records, but protects them based on the particular types of third parties that possess them.

Additionally, there are gaping holes in the statutory regime of protection, with classes of records not protected at all. Such records include those of merchants, both online and offline. Records held by bookstores, department stores, restaurants, clubs, gyms, employers, and other companies are not protected. Additionally, all the personal information amassed in profiles by database companies is not protected.

There is a significant amount of activity on the Internet that is not covered by the ECPA, such as information collected by websites. For example, consider In Re DoubleClick, Inc. Privacy Litigation, n407 where the court concluded that the use and access of cookies by DoubleClick did not violate the ECPA because the

"DoubleClick-affiliated Web sites had consented to DoubleClick's access of plaintiffs' communications to them." n408 Moreover, records maintained by Internet retailers and websites are often not considered "communications" under the ECPA.

Thus, the statutory regime is limited in its scope and has glaring omissions and gaps. Further, the statutes are often complicated and confusing, and their protection turns on technical distinctions that can leave wide fields of information virtually unprotected.

[*1149]

B. Statutory Regime Architecture: Structure

Even where the statutory regime applies, it is deficient in the procedures it adopts to regulate the government's access to third party records. The statutory regime permits information to be obtained via court order of subpoenas - a significant departure from the Fourth Amendment which generally requires warrants supported by probable cause to be issued by a neutral and detached magistrate.

Unlike warrants, subpoenas do not require probable cause and can be issued without judicial approval. Prosecutors, not neutral judicial officers, can issue subpoenas. n409 According to Stuntz: "While searches typically require probable cause or reasonable suspicion and sometimes require a warrant, subpoenas require nothing, save that the subpoena not be unreasonably burdensome to its target. Few burdens are deemed unreasonable." n410 According to Ronald Degnan, subpoenas are not issued "with great circumspection" and are often "handed out blank in batches and filled in by lawyers." n411 As Stuntz contends, federal subpoena power is "akin to a blank check." n412

Prosecutors can also use grand jury subpoenas to obtain third party records. n413 Grand jury subpoenas are "presumed to be reasonable" and may only be quashed if "there is no reasonable possibility that the category of materials the Government seeks will produce information relevant to the general subject of the grand jury investigation." n414 As Stuntz observes, grand jury subpoenas "are much less heavily regulated" than search warrants:

As long as the material asked for is relevant to the grand jury's investigation and as long as compliance with the subpoena is not too burdensome, the subpoena is enforced. No showing of probable cause or reasonable suspicion is necessary, and courts measure relevance and burden with a heavy thumb on the government's side of the scales. n415

[*1150] Therefore, courts "quash or modify" subpoenas only "if compliance would be unreasonable or oppressive." n416 Further, "judges decide these motions by applying vague legal standards case by case." n417

Court orders under most of the statutes are not much more constrained than subpoenas. They typically require mere "relevance" to an ongoing criminal investigation, a standard significantly lower and looser than probable cause.

The problem with subpoenas and court orders is that the judiciary has very limited oversight powers. The role of the judge in issuing or reviewing subpoenas is to determine the extent of the burden of producing the evidence. With this focus, financial hardship in producing information would give courts more pause when reviewing subpoenas than the potential invasions of privacy. The role of the judiciary in court orders is also quite restricted. For example, an order to install a pen register or trap and trace device under the ECPA merely requires that the applicant certify that the information sought be relevant to an ongoing criminal investigation. n418 Courts cannot look beyond the certification nor inquire into the truthfulness of the facts in the application. As one court has observed, the "judicial role in approving use of trap and trace devices is ministerial in nature." n419 In short, judicial involvement with subpoenas and court orders amounts to nothing more than a rubber stamp of judicial legitimacy.

In contrast, judges engage in a meaningful presearch review under the architecture of the Fourth Amendment.

Stronger standards force law enforcement officials to be more careful when applying for a warrant to engage in a search.

The current statutory regime that has attempted to fill the void created by the judicial evisceration of the Fourth Amendment is inadequate because it results in the de facto watering down of the warrant and probable cause requirements of the Fourth Amendment. As warrants supported by probable cause are replaced by subpoenas and court orders supported by "articulable facts" that are "relevant" to an investigation, the role of the judge in the process is diminished to nothing more than a decorative seal of approval. In many circumstances, neither court orders nor subpoenas are required. The government can simply ask for the information. An **[*1151]** individual's privacy is protected only by the vague and toothless privacy policies of the companies holding their information.

V. RECONSTRUCTING THE ARCHITECTURE

Today, much of our personal information is finding its way into the hands of third parties. Moreover, given the Court's current conception of privacy under the Fourth Amendment, the architecture of power that regulates many of the government's information-gathering practices is increasingly that of a confusing and gap-riddled statutory regime.

One solution to fill the void is for the Court to reverse Smith v. Maryland and United States v. Miller. Although Fourth Amendment architecture is significantly more protective than that of the statutory regime, the problem of how to regulate government access to third party records is not adequately addressed by Fourth Amendment architecture alone. As discussed earlier, the principal remedy for Fourth Amendment violations is the exclusionary rule, which prevents the government from introducing improperly obtained data during a criminal prosecution. However, many information-gathering abuses often occur in the absence of prosecutions. Therefore, the exclusionary rule is not sufficiently protective.

A better architecture of power to regulate government information-gathering from third parties should be constructed. In particular, such an architecture of power should prevent the types of problems associated with government information-gathering discussed earlier in Part II.C. An architecture should address minimization, particularization, and control. First, government information-gathering should be minimized. Sweeping investigations and vast stores of personal data in the hands of government entities present significant opportunities for the problematic uses discussed earlier. Second, efforts at gathering data should be particularized to specific individuals suspected of criminal involvement. Particularization requires law enforcement officials to exercise care in selecting the individuals who should be investigated, and it prevents dragnet investigations that primarily involve innocent people. One of the most important aspects of keeping the government under control is to prevent its investigatory powers from being turned loose on the population at large. Third, government information-gathering and use must be controlled. There must be some meaningful form of supervision over the government's information-gathering activity to ensure that it remains minimized and particularized. Further, government information uses must be controlled to prevent abuses, drifts in the uses of information, and security lapses.

[*1152] The aims of the architecture, however, are not the most difficult issue. Substantively, the architecture needs a scope. Which information-gathering activities should fall within the architecture's scope? Procedurally, the architecture needs a mechanism for carrying out its aims. What type of structural controls should an architecture adopt?

A. Scope: System of Records

An architecture begins with substance. It must provide guidance about which information-gathering activities it governs. What is the appropriate scope of an architecture regulating government information-gathering? In particular, should the architecture cover all instances where the government gathers personal data from third parties? Restricting all information gathering from third parties would prevent law enforcement officials from gathering initial information essential in developing sufficient evidence to establish probable cause. For example, witnesses and victims are third parties that have information about the defendant. If third parties are defined broadly, then the architecture could

constrain the police substantially, perhaps impeding their ability to interview people when investigating a crime. n420

Consequently, a line must be drawn to distinguish the instances where third parties can voluntarily supply information to the government and where the government will be prohibited from accessing information or otherwise be restrained prior to procuring the data. Although we may want to prevent Amazon.com from divulging to the government the log of books a person bought, we may not want to prohibit a person's neighbor or a stranger from telling the police which books she happened to observe the person reading.

An architecture must provide guidance for where the line is drawn. One way to draw the line is to focus on the type of data involved, distinguishing between "private" and "nonprivate" information. The architecture would protect all personal information that is private. However, how is privacy to be defined? The Court has defined privacy as total secrecy. But this conception excludes most information held by third parties from the scope of protection.

Another way to define private information is to focus on "intimate" information. A number of commentators have contended that intimacy is **[*1153]** the essential characteristic of privacy. For example, according to Julie Inness, "privacy's content covers intimate information, access, and decisions." n421 According to Tom Gerety, "intimacy is the chief restricting concept in the definition of privacy." n422 However, what constitutes "intimate" information? Without an adequate definition, "intimate" becomes nothing more than a synonym for "private." Commentators attempting to give substance to the word "intimacy" have defined the word too narrowly. For example, Jeffrey Reiman views intimate information as pertaining to certain kinds of loving and caring relationships. n423 Much private information, such as financial and health data, however, does not pertain to these types of relationships.

The more fundamental problem with focusing on whether information is private is that privacy is a product of context, not the status of particular facts. Easy distinctions such as intimate versus nonintimate and secret versus nonsecret fail to account for the complex nature of what is considered private. Privacy is a dimension of social practices, activities, customs, and norms that are shaped by history and culture. n424 The matters that are considered private and public have changed throughout history. Privacy is not a property of particular forms of information, since one can always lose privacy with respect to very sensitive and revealing facts about oneself. For example, the fact that a person has leprosy may be considered private information. But if that person becomes a public advocate for leprosy research and willingly announces to the public at large that she suffers from leprosy, the information is no longer private. Few would say that the fact that President Franklin Roosevelt suffered from polio remains a private matter today. Certainly, public disclosure does not eliminate the privacy of information; indeed, even information that is exposed to others may retain its private character. n425 Nevertheless, privacy depends upon degrees of accessibility of information, and under certain circumstances, even highly sensitive information may not be private.

[*1154] Additionally, focusing on the type of information does not solve the problem of distinguishing between the neighbor's tells the police what books he sees a person reading and Amazon.com's providing the police with a complete inventory of the books the person has purchased. By attempting to draw a line based upon the type of information, these two instances would be treated similarly. Another example more radically illustrates the problem. Many would deem information about a person's genitals to be private information. Should the police be required to obtain a warrant before talking to a victim of a sexual assault about an assailant's genitals? To many this would be absurd. On the other hand, many would express serious objections if the police, without probable cause, could simply compel information about a person's genitals from treating physicians.

Further, making distinctions based on the particular status of certain forms of information fails to account for what I call the "aggregation problem." This problem is caused by the accumulation of details. A fact here or there may seem innocuous but when combined, they become more telling about that person. Similar to a Seurat painting, where a multitude of dots juxtaposed together form a picture, bits of information when aggregated paint a portrait about a person.

Another way that a line could be drawn is based upon people's expectations. Such an approach would draw from

the Court's notion of "reasonable expectations of privacy." The problem with this approach, however, is that an empirical evaluation of expectations alone could gradually lead to the diminishment of privacy as more and more people come to expect that the records held by third parties can be readily obtained by the government. n426

If a line cannot be drawn based upon the type of information involved or people's expectations of privacy, then how should the line be drawn? The answer must focus on relationships. Privacy is not independent of the relationships of which it is a part. Individuals readily share information in certain private relationships, such as the family. In particular relationships people undertake certain risks including the risk of betrayal by one with whom confidences are shared. The fact that there are expectations and **[*1155]** risks, however, does not mean that they must be the exclusive focus of our inquiry.

The issue is not the conceivable risk of betrayal, but rather which risks people ought to assume and which risks people should be insured against. This determination has a normative dimension. When a patient discloses an ailment to a doctor, arguably the patient assumes the risk that the doctor will disclose the information to the public. However, there are several protections against this risk. First, patient-physician confidentiality is preserved by norms of professional conduct for physicians established by ethical rules. These rules include the Hippocratic Oath, which provides: "Whatever, in connection with my professional service, or not in connection with it, I see or hear, in the life of men, which ought not to be spoken of abroad, I will not divulge, as reckoning that all such should be kept secret." n427 Modern codes of medical ethics also require that physicians keep patient information confidential n428 or risk losing their licenses for improper disclosures. Patient-physician confidentiality is also protected in court with an evidentiary privilege. n429 Further, courts have created tort law causes of action against physicians who disclose personal information. n430 Finally, states have passed laws that protect against the disclosure of medical information. n431 Thus, in numerous ways, the law structures the patient-physician relationship to protect against the risk of disclosure. Similarly, the law of evidence has recognized the importance of protecting the privacy of communications between attorney and client, n432 priest and penitent, n433 husband and wife, n434 and psychotherapist and **[*1156]** patient. n435 Our expectations in these relationships are the product of both existing norms and the norm-shaping power of the law. As Christopher Slobogin notes, "in a real sense, we only assume those risks of unregulated government intrusion that the courts tell us we have to assume." n436

Therefore, the scope of the architecture should be shaped by considerations regarding social relationships. The architecture's scope should encompass all instances when third parties share personal information (in other words, information pertaining to individuals) contained within a "system of records." This term is taken from the Privacy Act, which defines a "system of records" as "a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual." n437 A "system of records" is used to distinguish between collecting information by speaking with specific individuals versus obtaining it through the vast stores of records held by companies.

The problems described in Part II stem from the nature of relationships with certain third parties and the problems of the government's collection and use of personal information. Therefore, the inquiry should focus on at least two sets of relationships: relationships with the government and relationships with the third parties that possess personal information.

In relationships with the government, the focus should be on what the collective society wants the government to be able to know rather than whether certain matters are public or private based on the extent of their exposure to others. The Court's conception of privacy assumes that the government stands in the same shoes as everybody else, which is clearly not the case. If we allow a loved one to read our diary, do we also want to the government to be able to read it? As Anthony Amsterdam has observed: "For the tenement dweller, the difference between observation by neighbors and visitors who ordinarily use the common hallways and observation by policemen who come into hallways to "check up' or "look around' is the difference between all the privacy that his condition allows and none." n438

[*1157] Indeed, the existence of Fourth Amendment limits indicates that the government stands in a different

position than ordinary citizens or private sector organizations. The possibility of aggregation and the rise of digital dossiers argue in favor of regulating the government's access to information.

One cannot lose sight of the fact that an architecture of power is being developed. The focus should be on the goals of the architecture rather than on technical distinctions over whether information is intimate enough or secret enough. These questions should not derail attention from the important issue of whether government information-gathering activities present sufficient actual and potential dangers to warrant protection. The problems discussed earlier regarding information flows from the private sector to the government stem from the extensiveness of the personal information that private sector entities are gathering today. Focusing on "systems of records" targets the type of information flow that raises concern. Because the problem of modern government information-gathering is caused by the increasing dossiers maintained in private sector record systems, the architecture targets those third parties that store data in record systems.

Our relationships with the entities that maintain record systems about us differ from other social relationships. Records are a more detailed and systematic form of information gathering. Though it is possible for the government to obtain personal data by interviewing friends and others, this is minimal compared to the systematic and profound sweep of information accessible through private sector record systems. The information in records is more permanent in nature and is readily aggregated. Thus, record systems are particularly dangerous because of their extensiveness and the ease with which information can be gathered, combined, stored, and analyzed.

Further, entities that maintain systems of records collect data in a power dynamic where information disclosure is often not consensual. A person can take considerable steps to prevent a stranger from gathering data without consent. For example, a person who is overzealous in gathering information can be subject to laws prohibiting stalking or harassment.

Relationships to employers and landlords, however, are different than those with our friends, neighbors, and even strangers. Currently, employers and landlords have a substantial amount of power to gather personal information. They often stand in an unequal position to that of the individual employees or tenants. The nature of the relationship with **[*1158]** employers and landlords provides them with a significantly greater amount of power and control with regard to information gathering. Moreover, the law often shapes these relationships to maintain or even further this disequilibrium of power.

Relationships with merchants and communications providers might not be as directly coercive as those with the entities that govern our livelihoods and dwellings. Because these relationships are more impersonal, perhaps it should be left to the market decide this issue. If consumers demand companies that protect their information from the government, then the market will reflect these choices.

Thus far, however, the market has not been responsive to this issue. As discussed earlier, privacy policies are often vague about information flows to the government. n439 Individuals are usually unaware of the extent to which information about them is collected. n440 As Edward Janger and Paul Schwartz point out, privacy is often a nonprice term in a negotiation that people do not adequately understand. In addition, the market fails to afford sufficient incentives to correct this information asymmetry. n441 Further, private sector entities have never established a relationship with the people whose data they have collected.

Even if people are informed, they have little choice but to hand over information to third parties. Life in the Information Age depends upon sharing information with a host of third party entities including phone companies, ISPs, cable companies, merchants, financial entities, medical and insurance providers, and so on. The Supreme Court in Smith and Miller has suggested that if people want to protect privacy, they should not share their information with third parties. However, refraining from doing so may result in people living as Information Age hermits, without credit cards, banks, Internet service, phones and television. The market does not seem to offer a wide array of choices for people on the basis of the amount of privacy they would like to protect. People rarely seem to bargain about privacy policies,

especially provisions about sharing information with the government. The policies are not individually negotiated, but are one-size-fits-all. According to Schwartz, this state of affairs is caused by the problem of "bounded rationality" in which people, "when faced with standardized terms, ... frequently accept whatever industry offers **[*1159]** them." n442 Given the current state of affairs, there is little hope that the market will achieve adequate protection alone.

Therefore, the scope of the architecture must be defined broadly to encompass any third party that maintains a "system of records." This definition of scope is not perfect, and there may be hard cases that call for exceptions. However, this rule would provide clear guidance to law enforcement officials when gathering information from third parties. This clarity is a virtue. Unlike the existing statutory architecture, which is complicated and often full of notable gaps, this architecture has clear and simple boundaries.

B. Structure: Regulated Subpoenas

Many different procedural mechanisms are available to control government information gathering. These mechanisms fall on a spectrum from no control over information-gathering on one end to complete restriction of it on the other. In the middle of the spectrum are mechanisms of oversight - where the government can access information only upon making certain showings before a neutral and external party who must authorize the access.

On the "no control" end of the spectrum, private sector entities may voluntarily disclose personal information to the government. If it so desired, Amazon.com could connect its computers to those of the FBI. If a private sector entity does not volunteer information, then the government can compel its production with a mere subpoena. The entity need not contest the subpoena or provide notice to the person to whom the information pertains. Whether the entity does so would be left up to market forces - to contracts between the entity and the consumer or privacy policies.

On the other end of the spectrum are architectural mechanisms of restriction - prohibitions on government collection and use of information. These mechanisms are embodied in the architecture of the Fifth Amendment and certain evidentiary privileges. The Fifth Amendment provides that "no person ... shall be compelled in any criminal case to be a witness against himself." n443 The Fifth Amendment's "privilege against self-incrimination" prevents the government from compelling individuals to testify against themselves, and completely bars use of the information **[*1160]** obtained in violation of the right at trial. In contrast, under the Fourth Amendment architecture, evidence is admissible at trial so long as the government obtains it pursuant to a valid search warrant.

The architecture of evidentiary privileges resembles in many respects the architecture of the Fifth Amendment, because privileges bar access to certain evidence altogether. Evidentiary privileges not only restrict the ability to obtain true information, but also the ability to present it at trial. As a result, privileges are sparingly recognized. For example, when independent prosecutor Kenneth Starr subpoenaed Monica Lewinsky's mother to testify against her daughter in front of a grand jury, there was a large public outcry at the tactic. n444 Although in many states, spouses may refuse to testify against each other in a criminal trial about confidential information that is known to the spouse, n445 most jurisdictions refuse to recognize a similar privilege for parents and children. n446

For certain relationships, complete restriction is necessary to protect the relationship. Where privacy is essential to the functioning of relationships that have a high social value, then the architecture of privileges is highly protective. Certain relationships depend upon the revelation of information. Privileges protect against "the general evil of infusing reserve and dissimulation, uneasiness, and suspicion and fear, into those communications which must take place." n447 As one court has noted, "by prearrangement with a criminal suspect's priest, minister or rabbi, psychiatrist or other physician, or lawyer, the police could obtain information of great value in combating crime. The only question is whether the price would be too high." n448 Certainly not all relationships that depend upon privacy are worth protecting. For example, criminal conspirators need privacy, but we do not consider the protection of these relationships to be socially beneficial. It is only those relationships that are important to society - such as the attorney-client and patient-physician relationships - that are protected by mechanisms of restriction.

Often, however, privacy is not essential to the relationship's existence, but is implicated in it. Exchange of information is incidental to most **[*1161]** commercial transactions and employment relationships. Adopting mechanisms of restriction to these relationships would herald a return to the regime of Boyd v. United States. n449

In Boyd, the Court held that the Fourth and Fifth Amendments prevented the government from issuing a subpoena to obtain a person's private papers. n450 Later, in Gouled v. United States, n451 the Court held that search warrants could not be used to gain access to one's "house or office or papers" merely to obtain evidence to use against that person in a criminal proceeding. n452 Under the rationale of Boyd and Gouled, the government could seize papers if they were instrumentalities of a crime or illegal contraband but not if they were merely evidence of a crime. This rule became known as the "mere evidence" rule.

The Boyd and Gouled regime has long been dismantled. The mere evidence rule was overturned in Warden v. Hayden, n453 where the Court eliminated the rule and permitted searches to find evidence of crimes. n454 Moreover, the Fifth Amendment was virtually eliminated as a protection against government access to personal information in records. In Shapiro v. United States, n455 the Court held that requiring a person to produce required records did not violate the Fifth Amendment. In Couch v. United States, n456 the government issued a subpoena to the defendant's accountant to obtain documents pertaining to its investigation of tax fraud. n457 The defendant challenged the subpoena on the basis that it violated his Fifth Amendment right against compulsory self-incrimination. n458 The Court rejected the challenge reasoning that "the Fifth Amendment privilege is a personal privilege: it adheres basically to the person, not to information that may incriminate him." n459 Because the subpoena was issued on a third party, "inquisitorial pressure or coercion against a potentially accused person, compelling her, against her will, to utter self-condemning words or produce incriminating documents is absent." n460 Likewise, in Fisher v. **[*1162]** United States, n461 the Court held that the Fifth Amendment privilege did not apply to subpoenas issued upon a person's attorney. n462 The Fifth Amendment, reasoned the Court, "protects against compelled self-incrimination, not the disclosure of private information." n463 In other words, according to the Court, the Fifth Amendment could not "serve as a general protector of privacy" and was limited to protecting against only the compulsion to testify against oneself. n464

Resurrecting the "mere evidence" rule and applying it to third party records would effectively bar the government from seeking and using records entirely unless they were the very instrumentalities through which a crime was perpetrated. This would cripple modern criminal investigation. As Stuntz observes: "Government regulation requires lots of information, and Boyd came dangerously close to giving regulated actors a blanket entitlement to nondisclosure. It is hard to see how modern health, safety, environmental, or economic regulation would be possible in such a regime." n465 Because Boyd rested in part on the Fifth Amendment, it completely prevented the government from obtaining and using the papers against the defendant no matter what procedure the government had used to obtain them.

In the middle of the spectrum are mechanisms of oversight. An architecture containing this type of mechanism is preferable to regulate government access of records held by third parties maintaining "systems of records." Mechanisms of oversight allow the government to gather information by making adequate showings before a neutral detached party. Oversight is embodied in the Fourth Amendment's per se warrant rule. The warrant requirement achieves the aims of minimization, particularization, and control. Collection is minimized by the requirement that the government justify that its information gathering is legitimate and necessary. The warrant ensures particularization with its requirement that there be probable cause that a particular person be engaged in criminal activity. Finally, the warrant achieves control (at least over the collection efforts) by having a neutral and detached party authorize the collection.

In many cases, warrants are the best regulatory device for government information-gathering. Often, at the point during an investigation that certain information from third parties becomes important for law **[*1163]** enforcement officials to obtain, there is already enough evidence to support a warrant. In both Smith and Miller there was probably sufficient evidence for the police to secure warrants. Therefore, the requirement of a warrant hopefully prevents cases of illegitimate abuses such as large-scale information sweeps and investigations without particularized suspicion, without unduly interfering with legitimate law enforcement activities. Further, third party records have few of the dangers that make warrants inefficient. For example, because third parties maintain the records, there are fewer opportunities for a

suspect to hide or destroy documents during the time law enforcement officials obtain a warrant.

However, as discussed above, merely applying the Fourth Amendment to government access to private sector records proves inadequate. First, is difficult to incorporate the "system of records" scope into the Fourth Amendment's reasonable expectations of privacy approach to determining the scope of protection. Second, the exclusionary rule only provides a remedy at trial, and many of the abuses associated with government information-gathering extend far beyond criminal trials.

Despite being far more permissive for government information-gathering purposes, subpoenas have certain protections not available with search warrants. Unlike warrants, they can be challenged prior to the seizure of the documents. The subpoenaed party can refuse to comply and make a motion to quash before a judge. Further, subpoenas permit the target to produce the documents rather than have government agents rummage through the party's home or belongings. n466 The advantages of subpoenas over search warrants are best illustrated in Zurcher v. The Stanford Daily, n467 where the police searched a newspaper's offices for evidence relating to a criminal suspect. The newspaper was not involved in the alleged crime; it merely possessed evidence. The Court upheld the search because it was made pursuant to a valid warrant. Dissenting justices contended that there were First Amendment concerns with such searches because they would disrupt newspaper operations and result in "the possibility of disclosure of information received from confidential sources, or of the identity of the sources themselves." n468 Congress responded to Zurcher by passing the Privacy Protection Act of 1980, n469 which restricts the use of search warrants for offices of newspapers and other media **[*1164]** entities for evidence of crimes of other parties. In effect, the Act requires the use of subpoenas rather than warrants to obtain such evidence.

The benefits of subpoenas, however, often do not apply to subpoenas for an individual's records issued on third parties because the third party does not need to notify the target or may not have any incentive to challenge the subpoena in court. n470 Further, as discussed before, subpoenas have many weaknesses compared to warrants, such as a lack of requiring particularized suspicion and little protection by way of oversight by the judiciary. n471

Therefore, the Fourth Amendment architecture should be resurrected statutorily, by heightening the standards required for the government to obtain a subpoena or court order. In this way, the statutory regime could require more stringent requirements for subpoenas and court orders, such as notice to the target and particularized suspicion. In other words, subpoenas and court orders could be strengthened to resemble warrants. This statutory regime would incorporate the exclusionary rule, a minimum statutory damages provision, and a framework by which to discipline offending law enforcement officials.

If subpoenas are not made identical to warrants, an alternative structural device, a "regulated subpoena," could be used. A regulated subpoena would be similar to a warrant. It would require notice to the third party from whom the records are sought and to the subject of the records being searched so that they may be able to contest the subpoena. In certain exigent circumstances, there may be exceptions to notice, as there are currently for warrants. n472

The regulated subpoena would require probable cause that the suspect is engaged in criminal activity. Specific records need not directly contain evidence of criminal activity but must be of "material importance" to the investigation. This differs from the standards often used by the statutory regime for subpoenas and court records in two respects. First, unlike the existing court order standard, where the person to whom the records pertain need not be involved in criminal activity at all, the regulated subpoena requires that the government demonstrate probable cause that the person is engaged in criminal activity. Second, unlike "relevance," the standard of **[*1165]** "material importance" is narrower. It is slightly more permissive than that of a warrant, which requires that the records contain evidence of criminal activity. However, unlike a warrant, the regulated subpoena can be challenged in court.

This approach is similar to courts' imposing heightened requirements when private parties seek to subpoena the identities of anonymous speakers. Consider, for example, Doe v. 2TheMart.com, n473 where the court held that a subpoena for the identities of anonymous speakers requires heightened standards to protect the right to speak

anonymously. n474 According to the court, four factors determine whether a subpoena can be issued:

(1) the subpoena seeking the information [must be] issued in good faith and not for any improper purpose, (2) the information sought relates to a core claim or defense, (3) the identifying information is directly and materially relevant to that claim or defense, and (4) information sufficient to establish or disprove that claim or defense is unavailable from other sources.

Other courts have articulated similar tests. n475 Even based on existing law, government subpoenas that compel information to reveal the identity of an anonymous speaker would seemingly fall within the reasoning of these courts and require heightened standards. However, a regulated subpoena would apply beyond situations where information is likely to affect anonymous speech to other forms of personal information.

The regulated subpoena requirement would contain certain exceptions. The general rule is that third parties maintaining personal information in a "system of records" cannot voluntarily disclose information to the government. Under compelling circumstances, however, third parties maintaining systems of records should be able to disclose facts voluntarily to the government. Compelling circumstances might include an imminent threat of harm to another. Another exception would allow the individual to whom the records pertain to authorize the government to obtain them from the third party without having to meet the heightened standards of the regulated subpoena. For example, if a victim of computer hacking wanted to permit the government to access the victim's ISP records, the victim could authorize the government to do so.

[*1166] Whether by reversing the third party doctrine, imposing Fourth Amendment restrictions on subpoenas, or restricting subpoenas via statute, the important point is that all of these approaches incorporate some of the central aspects of Fourth Amendment architecture: requiring a limitation in scope of the information that may be obtained and requiring meaningful external oversight.

C. Regulating Post-Collection Use of Data

The procedural architectural features discussed in the previous section are not sufficient to afford adequate protection to privacy. Another problem that must be addressed is the way personal information is used once it has been collected. As Stuntz astutely observes: "Fourth Amendment law regulates the government's efforts to uncover information, but it says nothing about what the government may do with the information it uncovers. Yet as the Clinton investigation shows, often the greater privacy intrusion is not the initial disclosure but the leaks that follow." n476 Carol Steiker notes: "Unlike other countries in North America and Western Europe, the United States [has] never developed a national plan to organize a "system' of policing or to provide for centralized control over police authority." n477 Once information is collected, the Fourth Amendment's architecture of oversight no longer applies. This is problematic, as many of the abuses of information by the government discussed earlier occur after the information has been collected.

The Privacy Act of 1974 n478 provides some limited regulation of records maintained by government law enforcement entities. However, the Act contains many exceptions and loopholes that have limited its effectiveness. Government entities can share information widely with each other. Further, information may be disclosed for any "routine use," an exception that many have criticized as a significant loophole. n479 As Robert Gellman astutely observes, the Privacy Act provides a "vague standard" that fails to serve as "a significant barrier to the sharing of personal information within agencies." n480 Additionally, the Act applies only to the federal government. Fewer than a third of the states have a privacy law similar to the Privacy Act. n481

[*1167] The Privacy Act is an important first step in reigning in the vast stores of data that government entities collect. There remains, however, much room for the Privacy Act to be improved and strengthened. One possible way to provide a safeguard is to mandate the destruction of data after certain periods of time or, mandate the transfer of data to

the judicial branch, after a certain period of time, for access only under special circumstances. Another way is to adopt a meaningful-purpose specification restriction. This means that, with certain reasonable exceptions, information collected from third party records may only be used for the particular purpose for which it is collected.

VI. CONCLUSION

One of the most significant threats to privacy of our times, government information-gathering and-use, is inadequately regulated. The Court's Fourth Amendment jurisprudence has been mired in the difficulties of conceptualizing privacy, thus preventing the application of the Fourth Amendment. A statutory regime has arisen to fill the void, but it is severely flawed. A new architecture of power must be constructed, one that effectively regulates the government's collection and use of third party records. This task is not easy in a rapidly changing society that is adjusting to the profound new dimensions of the Information Age. This Article is thus a beginning of the process.

Legal Topics:

For related research and practice materials, see the following legal topics:
Computer & Internet LawCopyright ProtectionCivil Infringement ActionsDefensesGeneral OverviewCriminal Law & ProcedureSearch & SeizureSearch WarrantsProbable CauseGeneral OverviewGovernmentsFederal GovernmentDomestic Security

FOOTNOTES:

n1. See infra Part II.

n2. See infra Part II.

n3. See infra Part II.

n4. Government access to such data may implicate one's First Amendment rights to freedom of speech and freedom of association. See infra Part II.C.

n5. See, e.g., David H. Flaherty, Protecting Privacy in Surveillance Societies (1989); Paul M. Schwartz & Joel R. Reidenberg, Data Privacy Law 39 (1996); ("Totalitarian regimes in Eastern Europe relied on information gathering and data storage to weaken the individual capacity for critical reflection and to repress any social movements outside their control."); Paul M. Schwartz, Privacy and Participation: Personal Information and Public Sector Regulation in the United States, 80 Iowa L. Rev. 553, 560 (1995); Peter P. Swire, Financial Privacy and the Theory of High-Tech Government Surveillance, 77 Wash. U. L.Q. 461, 471 (1999) (articulating problems of "how an authoritarian or totalitarian government might use and abuse information about citizens'

financial transactions").

n6. See generally Paul M. Schwartz, Internet Privacy and the State, 32 Conn. L. Rev. 815 (2000); Paul M. Schwartz, Privacy and Democracy in Cyberspace, 52 Vand. L. Rev. 1609 (1999).

n7. I previously explored the contrast between these two types of power in the context of private sector information collection and use. See Daniel J. Solove, Privacy and Power: Computer Databases and Metaphors for Information Privacy, 53 Stan. L. Rev. 1393 (2001).

n8. See infra Part III.

n9. Olmstead v. United States, 277 U.S. 438, 479 (1928) (Brandeis, J., dissenting).

n10. Schmerber v. California, 384 U.S. 757, 767 (1966).

n11. See, e.g., Smith v. Maryland, 442 U.S. 735, 743 (1979); United States v. Miller, 425 U.S. 435, 444 (1976). For a more extensive discussion of these cases and others, see infra Part III.C.

n12. See infra Part IV.

n13. 277 U.S. 438, 464 (1928).

n14. For a discussion of the ineffectiveness of 605, see infra Part IV.A.1.

n15. See infra Part III.B.

n16. Katz v. United States, 389 U.S. 356, 356 (1967).

n17. Elsewhere, I contend that privacy must be conceptualized in a multifaceted way, from the bottom-up by focusing on social practices rather than a rigid category with a single unifying essence or common denominator. See Daniel J. Solove, Conceptualizing Privacy, 90 Cal. L. Rev. 1087, 1088-99 (2002).

n18. See infra Part III.C.

n19. Lawrence Lessig has popularized the term "architecture" to refer to technological systems of governance - the way that computer code structures what we can do and how we act in cyberspace. See generally, Lawrence Lessig, Code and Other Laws of Cyberspace (1999) [hereinafter Code]; Lawrence Lessig, The Architecture of Privacy, 1 Vand. J. Ent. L. & Prac. 56 (1999). I use this term more broadly than Lessig does, to refer to a particular power structure, not merely created by computer code or technology, but by the law. Although certainly not antagonistic to law, Lessig's view of privacy privileges technological to legal architecture. According to Lessig, law merely sets the default entitlements to information, and technological architectures do the rest. See id. at 160-61. However, I believe that law has a much larger role to play in the protection of privacy. Solove, supra note 7, at 1445-55.

n20. See Robert O'Harrow, Jr., Intricate Screening of Flyers In Works: Database Raises Privacy Concerns, Wash. Post., Feb. 1, 2002, at A1.

n21. See Cal. Bankers Ass'n v. Shultz, 416 U.S. 21, 85 (1974) (Douglas, J. dissenting) ("In a sense a person is defined by the checks he writes. By examining them the agents get to know his doctors, lawyers, creditors, political allies, social connections, religious affiliation, educational interests, the papers and magazines he reads, and so on ad infinitum.").

n22. See Dana Hawkins, Gospel of a Privacy Guru: Be Wary; Assume the Worst, U.S. News & World Rep., June 25, 2001, http://www.usnews.com/usnews/nycu/tech/articles/010625/tech/privacy.htm (describing hotel chain sharing lists of the movies, including pornographic ones, customers pay to watch in their hotel rooms).

n23. Julia Scheeres, No Thumbprint, No Rental Car, Wired News, Nov. 21, 2001, at http://wired.com/news/print/0,1294,48552,00.html.

n24. See, e.g., Paul M. Schwartz, Beyond Lessig's Code for Internet Privacy: Cyberspace Filters, Privacy-Control, and the Fair Information Practices, 2000 Wisc. L. Rev. 743, 770-71 (describing lack of employee privacy).

n25. See Dana Hawkins, Digital Skulduggery, U.S. News & World Rep., Oct. 2, 2000 at 64. For a detailed account of privacy in the workplace, see generally, John D.R. Craig, Privacy and Employment Law (1999).

n26. J.C. Conklin, Under the Radar: Content Advisor Snoops as Workers Surf Web, Wall St. J., Oct. 15, 1998, at B8.

n27. See Baggs v. Eagle-Pitcher Indus., Inc., 750 F. Supp. 264, 272-73 (W.D. Mich. 1990) (holding no tort or contract remedies for at-will employee discharged for refusing to take a drug test). For an excellent discussion of the issue, see generally, Pauline T. Kim, Privacy Rights, Public Policy, and the Employment Relationship, 57 Ohio St. L.J. 671 (1996).

n28. This information was requested in employer questionnaires in American Federation of Government Employees v. HUD, 118 F.3d 786 (D.C. Cir. 1997) and Walls v. City of Petersburg, 895 F.2d 188 (4th Cir. 1990). The Americans With Disabilities Act (ADA), 42 U.S.C. 12112 prevents inquiries of an applicant regarding disabilities; however, inquiries can be made "into the ability of an applicant to perform job related functions." 42 U.S.C. 12112(d)(2)(B) (2002). An employer may require all entering employees to undergo a medical examination. 12112(d)(3).

n29. See Sarah Schafer, Searching for a Workable Fit; Employers Try Psychological Tests to Help with More than the Right Hire, Wash. Post, Jan. 14, 1999, at V5.

n30. See Solove, Privacy and Power, supra note 7, at 1408-09.

n31. See id. at 1406-10.

n32. Catalina Marketing Corp. has collected information about the supermarket purchases of thirty million households. See Robert O'Harrow, Jr., Behind the Instant Coupons, a Data-Crunching Powerhouse, Wash. Post., Dec. 31, 1998, at A20.

n33. Although the rise of the Internet promises to herald a new age of freedom, there is a dark side to the Internet, where instead of a world of freedom, it is becoming a realm of domination and control. As Lawrence Lessig observes: "Cyberspace does not guarantee its own freedom but instead carries an extraordinary potential for control." Lessig, Code, supra note 19, at 58.

n34. See, e.g., United States v. Hambrick, 55 F. Supp. 2d 504, 505 (W.D. Va. 1999) (obtaining from ISP the identity of a pseudonymous individual in an Internet chat room); United States v. Charbonneau, 979 F. Supp. 1177, 1179 (S.D. Ohio 1997) (obtaining the identity of an pseudonymous Internet user from ISP); State v. Schroeder, 613 N.W.2d 911, 913 (Wis. Ct. App. 2000) (obtaining from ISP the identity of individual who posted sexually suggestive comments on the Internet about another individual).

n35. See 18 U.S.C. 2703(c) (2000), as amended by the USA-PATRIOT Act 210-11.

n36. 983 F. Supp. 215, 217 (D.D.C. 1998).

n37. When he called AOL, the official did not identify himself as a Navy official but instead stated that he had received a fax from a pseudonymous individual and that he wanted to find out the identity of the individual. The AOL representative identified the individual.

n38. Jerry Kang, Information Privacy in Cyberspace Transactions, 50 Stan. L. Rev. 1193, 1199 (1998).

n39. See Julie E. Cohen, The Right to Read Anonymously: A Closer Look at "Copyright Management" in Cyberspace, 28 Conn. L. Rev. 981, 983 (1996) ("The same technologies that enable readers to access digitally stored works, however, also will enable copyright owners to generate precise and detailed records of such access."); Schwartz, Internet Privacy and the State, supra note 6, at 849 (noting that copyright management "systems enable copyrighted works themselves to carry out a pervasive monitoring of individual activity"). See

also Pamela Samuelson, Will the Copyright Office Be Obsolete in the Twenty-First Century?, 13 Cardozo Arts & Ent. L.J. 58 (1994).

n40. See Solove, Privacy and Power, supra note 7, at 1411-12.

n41. See id. at 1411.

n42. See Robert O'Harrow, Jr., Fearing a Plague of "Web Bugs'; Invisible Fact-Gathering Code Raises Privacy Concerns, Wash. Post, Nov. 13, 1999, at E1; Leslie Walker, Bugs That Go Through Computer Screens, Wash. Post, Mar. 15, 2001, at E1.

n43. J.D. Lasica, The Net NEVER Forgets, Salon, Nov. 25, 1998, at http://www.salon.com/21st/feature/1998/11/25feature.html.

n44. For a discussion of the types of information collected by health websites, see Pew Internet & American Life Project, Exposed Online: Why the New Federal Health Privacy Regulation Doesn't Offer Much Protection to Internet Users (Nov. 2001), at http://www.pewinternet.org.

n45. Id.

n46. This feature is available on Amazon.com at http://www.amazon.com.

n47. For example, Yahoo!, at http://www.yahoo.com, offers a personalized web page service.

n48. See http://calendar.msn.com/CalendarNorm.html.

n49. See Jim Sterne, What Makes People Click: Advertising on the Web, 238-41 (1997); Solove, Privacy and Power, surpa note 7, at 1412.

n50. See Daniel J. Solove, Access and Aggregation: Privacy, Public Records, and the Constitution, 86 Minn. L. Rev. (forthcoming 2002).

n51. See generally Joel R. Reidenberg, Resolving Conflicting International Data Privacy Rules in Cyberspace, 52 Stan. L. Rev. 1315 (2000); Joel R. Reidenberg, Setting Standards for Fair Information Practice in the U.S. Private Sector, 80 Iowa L. Rev. 497 (1995).

n52. See generally Solove, Privacy and Power, supra note 7.

n53. See generally Solove, Access and Aggregation, supra note 50.

n54. Fed. Trade Comm'n, Individual Reference Services 1, 27-28 (1997), available at 1997 WL 784156, at 9.

n55. See Glenn R. Simpson, Big Brother-in-Law: If the FBI Hopes to Get the Goods on You, It May Ask ChoicePoint, Wall St. J., Apr. 13, 2001, at A1.

n56. See id.

n57. See Jeffrey Benner, The Army is Watching Your Kid, Wired News, Jan. 29, 2001, at http://www.wired.com/news/print/0,1294,41476,00.html.

n58. See infra Part IV.

n59. See infra Part IV.

n60. Daniela Deane, Legal Niceties Aside ... ; Federal Agents Without Subpoenas Asking Firms for Records, Wash. Post, Nov. 7, 2001, at E1.

n61. The Attorney General's Guidelines on General Crimes, Racketeering Enterprise and Domestic Security/Terrorism Investigations II.C.1 (March 21, 1989).

n62. See The Attorney General's Guidelines on General Crimes, Racketeering Enterprise and Terrorism Enterprise Investigations VI (May 30, 2002).

n63. Id.

n64. Id. at VI.B.1. See also Susan Schmidt & Dan Eggen, FBI Given More Latitude: New Surveillance Rules Remove Evidence Hurdle, Wash. Post, May 30, 2002, at A1.

n65. In particular, Starr was interested in discovering if Lewinsky had purchased Nicholson Barker's Vox, a novel that pertained to phone sex. See Mike Feinsilber, Bookstore Refuses to Comply with Starr's Subpoena for Lewinsky Book List, Nando Times News (1998), http://archive.nandotimes.com/newsroom/nt/529nonono.html.

n66. See id.

n67. Felicity Barringer, Using Books as Evidence Against Their Readers, N.Y. Times, Apr. 8, 2001, at WK3; Justin Rickard, Police vs. Bookstore in Privacy Rights Case, (Dec. 16, 2000), at http://www.privacyfoundation.org/resources/bookstore.asp. See also Our Books Are Our Business, ABCnews.com, at http://my.abcnews.go.com/2020<uscore>020216<uscore>bookstores<uscore>feature.htm. The technique of obtaining information from bookstores has escalated since the Monica Lewinsky episode. In 2000-01, prior to September 11, Borders bookstores in Massachusetts and Kansas were searched and subpoenaed. See Barringer, supra, at WK3. In the Tattered Cover case, the Colorado Supreme Court recently sided with the bookstore. See Tattered Cover, Inc. v. City of Thornton, 44 P.3d 1044 (Colo. 2002).

n68. Barringer, supra note 67.

n69. Lisa Guernsey, What Did You Do Before the War?, N.Y. Times, Nov. 22, 2001, at G1. See also Victor Schachter & Trey Wichmann, The Aftermath of September 11: No Longer Business as Usual for Security, Safety to Privacy in the Workplace, in Third Annual Institute Privacy Law: New Developments & Issues in a Security Conscious World 623, 627 (Francoise Gilbert, John B. Kennedy & Paul M. Schwartz eds. 2002) (describing increase in employer scrutiny of applicants' backgrounds).

n70. Elinor Mills Abreu, SafeWeb Shuts Free Anonymous Web Service, Infowar.com, Nov. 11, 2001, at http://www.infowar.com/class<uscore>1/01/class1<uscore>112001a<uscore>j.shtml.

n71. See Paul Beckett, Big Banks, U.S. Weigh Pooling Data on Terror, Wall St. J., Nov. 26, 2001, at A2; Robert O'Harrow, Jr., Financial Database to Screen Accounts: Joint Effort Targets Suspicious Activities, Wash. Post, May 30, 2002, at E1.

n72. See David E. Rosenbaum, A Nation Challenged: Questions of Confidentiality, N.Y. Times, Nov. 22, 2001, at B7.

n73. See infra Part IV.

n74. See infra Part IV.

n75. See Mike Snider, Privacy Advocates Fear Trade-Off for Security; FBI Sends Warrants to Service Providers, USA Today, Sept. 13, 2001, at D8.

n76. See Robert Lemos, FBI Taps ISPs in Hunt for Attackers, ZD Net Sept. 12, 2001, at http://zdnet.com/filters/printerfriendly/0,6061,5096919-2,00.html.

n77. E. Judson Jennings, Carnivore: U.S. Government Surveillance of Internet Transmissions, 6 Va. J. L. & Tech. 10, PP 49, 96 (2001).

n78. The USA-PATRIOT Act enshrined the FBI's Carnivore device into law. USA-PATRIOT Act 216, codified at 18 U.S.C. 3133(a)(3) (1994).

n79. MSN Statement of Privacy, at http://privacy.msn.com.

n80. Amazon.com Privacy Notice, at http://www.amazon.com.

n81. Privacy Policy, at http://pages.ebay.com/help/community/png-priv.html.

n82. Model Privacy Statement, at http://truste.com/bus/pub<uscore>sample.html.

n83. See id.

n84. See id.

n85. For example, Larry Ellison, the CEO of Oracle Corporation, proposed a system of national identification involving biometrics. See Larry Ellison, Digital IDs Can Help Prevent Terrorism, Wall St. J., Oct. 8, 2001, at A26.

n86. See Greg Schneider & Robert O'Harrow, Jr., Pentagon Makes Rush Order for Anti-Terror Technology, Wash. Post, Oct. 26, 2001, at A10.

n87. Robert O'Harrow, Jr., Drivers Angered over Firm's Purchase of Photos, Wash. Post, Jan. 28, 1999, at E1; Robert O'Harrow, Jr. & Liz Leyden, U.S. Helped Fund Photo Database of Driver IDs: Firm's Plan Seen as Way to Fight Identity Crime, Wash. Post, Feb. 18, 1999, at A1.

n88. 31 U.S.C. 1081 (1994).

n89. H. Jeff Smith, Managing Privacy 24 (1994).

n90. 31 U.S.C. 1081.

n91. See 31 C.F.R. 103.22(1). In California Bankers Association v. Shultz, 416 U.S. 21, 67-69 (1974), the Court held that the bankers lacked standing to challenge the regulations. Shultz effectively resolved the Fourth Amendment rights of the individuals with accounts at the bank. Id. According to the third party doctrine, these individuals have no reasonable expectation of privacy in their bank records. Id.

n92. See Personal Responsibility and Work Opportunity Reconciliation Act of 1996, Pub. L. No. 104-193, 110 Stat. 2105 (1996). See generally Robert O' Harrow, Jr., Uncle Sam Has All Your Numbers, Wash. Post, June 27,1999, at A1.

n93. Pub. L. 103-414, 108 Stat. 4279 (1994).

n94. See United States Telecom Ass'n v. FCC, 227 F.3d 450, 454 (D.C. Cir. 2000).

n95. See Solove, Privacy and Power, supra note 7, at 1393.

n96. See generally George Orwell, Nineteen Eighty-Four (1949).

n97. See Solove, Privacy and Power, supra note 7, at 1417-19.

n98. See Margaret Raymond, Rejecting Totalitarianism: Translating the Guarantees of Constitutional Criminal Procedure, 76 N.C. L. Rev. 1193, 1198 (1998).

n99. See Schwartz, Privacy and Democracy in Cyberspace, supra note 6, at 1658-59.

n100. Id. at 1664.

n101. Id. at 1665.

n102. Id. at 1657.

n103. See id. at 1651-52.

n104. NAACP v. Alabama, 357 U.S. 449, 462 (1958).

n105. See, e.g., Shelton v. Tucker, 364 U.S. 479, 489 (1960) (holding unconstitutional a law requiring teachers to disclose membership in organizations); NAACP, 357 U.S. at 466 (restricting compelled disclosure of membership lists of NAACP).

n106. 401 U.S. 1 (1971).

n107. Id. at 6.

n108. It is unclear how receptive the Court will be to this argument. The Court has held that mere information gathering about a group's public activities did not harm First Amendment interests enough to give rise to standing. See Laird v. Tatum, 408 U.S. 1, 12-15 (1972).

n109. 362 U.S. 60, 63-64 (1960).

n110. Id. at 64.

n111. Id. at 65.

n112. 514 U.S. 334, 334 (1995).

n113. Id. at 342.

n114. See, e.g., Doe v. 2TheMart.com, Inc., 140 F.Supp.2d 1088, 1093-95 (W.D. Wash. 2001); Columbia Insurance Co. v. Seescandy.com, 185 F.R.D. 573, 578-80 (N.D. Cal. 1999).

n115. Cohen, supra note 39, at 1012.

n116. Recently, the Colorado Supreme Court in Tattered Cover, Inc. v. City of Thornton, 44 P.3d 1044, 1044 (Colo. 2002), concluded that heightened scrutiny should apply to instances where police use a search warrant to seek records of a person's book purchases at bookstores. The holding was premised under Colorado's constitution:

We turn to our Colorado Constitution, which we now hold requires a more substantial justification from the government than is required by the Fourth Amendment of the United States Constitution when law enforcement officials attempt to use a search warrant to obtain an innocent, third-party bookstore's customer purchase records.

Id. at 1056. The court's holding was premised on a recognition that police searches of bookstores could chill bookstore customers' First Amendment rights to read anonymously: "When a person buys a book at a bookstore, he engages in activity protected by the First Amendment because he is exercising his right to read and receive ideas and information. Any governmental action that interferes with the willingness of customers to purchase books, or booksellers to sell books, thus implicates First Amendment concerns." Id. at 1052. The court concluded that "law enforcement officials must demonstrate a sufficiently compelling need for the specific customer purchase record sought from the innocent, third-party bookstore." Id. at 1058.

n117. David J. Garrow, The FBI and Martin Luther King, Jr. 18 (1980).

n118. See generally Curt Gentry, J. Edgar Hoover: The Man and the Secrets (1991); Richard Gid Powers, Secrecy and Power: The Life of J. Edgar Hoover (1987).

n119. See Silas J. Wasserstrom & Louis Michael Seidman, The Fourth Amendment as Constitutional Theory, 77 Geo. L.J. 19, 82 (1988); William J. Stuntz, The Substantive Origins of Criminal Procedure, 105 Yale L.J. 393, 408 (1995).

n120. Lawrence M. Friedman, Crime and Punishment in American History 27 (1993).

n121. Carol S. Steiker, Second Thoughts About First Principles, 107 Harv. L. Rev. 820, 830-31 (1994).

n122. See Stuntz, supra note 119, at 401.

n123. See id.

n124. See, e.g., Friedman, supra note 120, at 67; David R. Johnson, Policing the Urban Underworld: The Impact of Crime on the Development of the American Police 1800-1887, at 9 (1979); Eric Monkkonen, Police in Urban America, 1860-1920, at 42-44 (1981); Stuntz, supra note 119, at 435.

n125. Gentry, supra note 118, at 112. The organization created in 1908 was called the Bureau of Investigation (BI); it became the FBI in 1935. See id. at 113.

n126. Id. at 111-12.

n127. See, e.g., Albert J. Reiss, Jr., Police Organization in the Twentieth Century, in Modern Policing 51, 68-82 (Michael Tonry & Norval Morris eds., 1992). Reiss points out that one of the distinctive and unique facets of law enforcement bureaucracy in the United States "is that the greatest discretionary powers are lodged with the lowest-ranking officials in the system and that most discretionary decisions are not made a matter of record." Id. at 74.

n128. See, e.g., Whitfield Diffie & Susan Landau, Privacy on the Line: The Politics of Wiretapping and Encryption 118 (1998) ("Police forces today not only have access to nationwide (and often worldwide) records, but much of that access is directly available to officers in the field.").

n129. See Stuntz, supra note 119, at 408.

n130. It is virtually undisputed that one of the central reasons the Framers created the Fourth Amendment was to guard against the use of general warrants. See, e.g., Leonard W. Levy, Origins of the Bill of Rights 158 (1999); Tracey Maclin, When the Cure for the Fourth Amendment Is Worse than the Disease, 68 S. Cal. L. Rev. 1, 9 (1994).

n131. California Bankers Ass'n v. Shultz, 416 U.S. 21, 85 (1974) (Douglas, J. dissenting).

n132. For a discussion of the harms of a national identification system, see Richard Sobel, The Degradation of Political Identity Under a National Identification System, 8 B.U. J. Sci. & Tech. L. 37 (2002). See also Solove, Access and Aggregation, supra note 50.

n133. Diffie & Landau, supra note 128, at 138.

n134. See id. at 143.

n135. See id. at 146; Barringer, supra note 67, at WK3.

n136. See Diffie & Landau, supra note 128, at 143.

n137. Although the Army's surveillance efforts were challenged before the Supreme Court on First Amendment grounds in Laird v. Tatum, 408 U.S. 1, 1 (1972), the Court concluded that the targets of the information gathering lacked standing because they only alleged "generalized yet speculative apprehensiveness that the Army may at some future date misuse the information in some way that would cause direct harm to [them]." Id. at 13.

n138. Id.

n139. See id. at 7.

n140. See Philadelphia Yearly Meeting of the Religious Society of Friends v. Tate, 519 F.2d 1335, 1335 (3d Cir. 1975).

n141. See Priscilla M. Regan, Legislating Privacy 86 (1995); Robert Gellman, Does Privacy Law Work?, in Technology and Privacy: The New Landscape 193, 198 (Philip E. Agre & Marc Rotenberg, eds., 1997).

n142. See Gary T. Marx, UnderCover: Police Surveillance in America 209-10 (1988).

n143. See Computer Matching and Privacy Protection Act (CMPPA) of 1988, Pub. L. No. 100-503, 102 Stat. 2507, codified as amended at 5 U.S.C. 552a(a)(8)-(13), e(12), (o)-(r), (u). The CMPPA requires agencies to formulate procedural agreements before exchanging computerized record systems and establishes Data Integrity Boards within each agency. See id. The CMPPA establishes Data Integrity Boards within each agency to

oversee matching, requires agencies to perform a cost-benefit analysis of proposed matching endeavors, and requires agencies to notify individuals of the termination of benefits due to computer matching and to permit individuals an opportunity to refute the termination. See id.

n144. See Gen. Accounting Office, Computer Matching: Quality of Decisions and Supporting Analyses Little Affected by 1988 Act (1993); Schwartz & Reidenberg, supra note 5, at 101; Information Policy Committee, National Information Infrastructure Task Force, Options for Promoting Privacy on the National Information Infrastructure: Draft for Public Comment 15 (Apr. 1997); Schwartz, Privacy and Participation, supra note 5, at 588 (noting that CMPPA "creates no substantive guidelines to determine when matching is acceptable").

n145. See Regan, supra note 141, at 90.

n146. Pamela Samuelson, Privacy as Intellectual Property?, 52 Stan. L. Rev. 1125, 1143 (2000). See also David H. Flaherty, Protecting Privacy in Surveillance Societies 373-74 (1989).

n147. Eric. K. Yamamoto, Margaret Chon, Carol I. Izumi, Jerry Kang, & Frank H. Wu, Race, Rights, and Reparations: Law and the Japanese American Internment 38 (2001).

n148. See id. at 96.

n149. See id. at 38-39. See also Daniel J. Solove, The Darkest Domain: Deference, Judicial Review, and the Bill of Rights, 84 Iowa L. Rev. 941, 941 (1999). See generally Eugene V. Rostow, The Japanese American Cases - A Disaster, 54 Yale L.J. 489 (1945).

n150. Diffie & Landau, supra note 128, at 138. See also David Burnham, The Rise of the Computer State 24 (1983).

n151. Frank J. Donner, The Age of Surveillance: The Aims and Methods of America's Political Intelligence System 33 (1980).

n152. See Gentry, supra note 118, at 76. Most of the letter bombs were halted at the Post Office due to inadequate postage. See id.

n153. See Charles H. McCormick, Seeing Reds: Federal Surveillance of Radicals in the Pittsburgh Mill District, 1917-1921, 120 (1997); Powers, supra note 118, at 69.

n154. See McCormick, supra note 153, at 103.

n155. See Donner, supra note 151, at 34; Gentry, supra note 118, at 79; Powers, supra note 118, at 68.

n156. See Gentry, supra note 118, at 93.

n157. See Powers, supra note 118, at 79-80.

n158. See Gentry, supra note 118, at 98-99.

n159. See Ellen Schrecker, The Age of McCarthyism: A Brief History with Documents 92-94 (1994).

n160. Id. at 10.

n161. Gentry, supra note 118, at 378-80, 402; Powers, supra note 118, at 320-21.

n162. See Schrecker, supra note 159, at 76-84. For further background about the McCarthy era, see

generally Albert Fried, McCarthyism: The Great American Red Scare: A Documentary History (1997) and Richard M. Fried, Nightmare in Red: The McCarthy Era in Perspective (1990).

n163. Powers, supra note 118, at 321.

n164. See Schrecker, supra note 159, at 77.

n165. See Seth I. Kreimer, Sunlight, Secrets, and Scarlet Letters: The Tension Between Privacy and Disclosure in Constitutional Law, 140 U. Pa. L. Rev. 1, 13-71 (1991).

n166. Schrecker, supra note 159, at 76-84.

n167. See M.L. Elrick, Cops Abuse Database, 3 Privacy Suits Say They Charge Officers Use LEIN to Check Out Personal Matters, Detroit Free Press, Dec. 25, 2001, at A1.

n168. See id.

n169. See id.

n170. For an excellent discussion of Napster and the impact of copyright law on music sharing, see generally Raymond Shih-Ray Ku, The Creative Destruction of Copyright: Napster and the New Economics of Digital Technology, 69 U. Chi. L. Rev. 263 (2002).

n171. See Joseph Bensman & Robert Lilienfeld, Between Public and Private: The Lost Boundaries of the Self 97 (1979) ("Large-scale organizations tend to invade privacy ...in order to use the information so gained as a private means to secure its public goals and in part by using managed leaks to reveal the private vices of their organizational and personal enemies.").

n172. Charles J. Sykes, The End of Privacy: Personal Rights in the Surveillance Society 160 (1999). See Diffie & Landau, supra note 128, at 163 (wiretapping of members of Congress and Supreme Court Justices); Gentry, supra note 118 (providing detailed description of Hoover's collection of files and extensive wiretapping).

n173. See Garrow, supra note 117, at 165.

n174. See, e.g., Diffie & Landau, supra note 128, at 140-42. It was not until 1975, nearly a decade after the wiretapping and three years after Hoover's death, that Congress conducted an inquiry into the wiretapping of King through the famous Church Committee. See id. at 178.

n175. Garrow, supra note 117, at 100-01.

n176. See id. at 102 passim.

n177. Id. at 126.

n178. Id. at 26.

n179. See id. at 78. Hoover's dislike of King may have also stemmed from racism. It is well-documented that Hoover was racist. See id. at 153.

n180. See id. at 79-83.

n181. See id. at 151. According to Garrow, the investigation and electronic surveillance of King in 1962-63 began as an inquiry into King's ties with Levison; in 1963-64, the investigation turned to an effort to discredit and attack King.

n182. See generally Thomas A. Markus, Buildings and Power: Freedom and Control in the Origin of Modern Building Types (1993). One of the most famous examples of the way architecture can affect social structure is the Panopticon, an architectural design for a prison developed by Jeremy Bentham. According to this design, prison cells are arranged around a central observation tower, from which all cells are visible. However, those in the cells cannot observe if anybody is in the tower. The goal of this architecture is for each prisoner to believe that at any moment, she could be being watched, and this belief will result in increased obedience. As Michel Foucault aptly noted, the Panopticon can be replicated in our society in ways not merely limited to physical architecture. Panoptic architecture can be part of the structure of social relationships. See Michel Foucault, Discipline and Punish: The Birth of the Prison 200-05 (Alan Sheridan Trans. 1977).

n183. Neal Kumar Katyal, Architecture as Crime Control, 111 Yale L.J. 1039 (2002).

n184. For an extensive discussion of how privacy relates to social practices, see Solove, supra note 17, at 1126-43.

n185. See, e.g., Minnesota v. Carter, 525 U.S. 83, 99 (1998) (Kennedy, J., concurring) ("Fourth Amendment protection ... is in essence a personal right."); Whalen v. Roe, 429 U.S. 589, 599-00 (1977) (privacy is an "individual interest in avoiding disclosure of personal matters"); Restatement (Second of Torts 652(I) comment (a) (stating that "the right protected by the action for invasion of privacy is a personal right, peculiar to the individual whose privacy is invaded"); Ellen Alderman & Caroline Kennedy, The Right to Privacy xv (1995) (noting that "privacy is, by definition, a personal right"); William M. Beaney, The Right to Privacy and American Law, 31 Law & Contemp. Probs. 253, 254 (1966) (observing that "the right to privacy is an affirmation of the importance of certain aspects of the individual person and his desired freedom from unreasonable intrusive conduct by others").

n186. John Dewey, The Future of Liberalism, in 11 Later Works 290 (Jo Ann Boydston ed. 1991).

n187. See, e.g., John Dewey, Experience and Nature 162-63 (1925); Dewey, Liberalism and Social Action 7 (1935).

n188. John Dewey, Liberalism and Civil Liberties, in 11 Later Works 374 (Jo Ann Boydston ed. 1991).

n189. Garrow, supra note 117, at 209.

n190. See U.S. Const. amend. V.

n191. U.S. Const. amend. IV.

n192. See generally Akhil Reed Amar, The Constitution and Criminal Procedure (1997); Silas J. Wasserstrom, The Fourth Amendment's Two Clauses, 26 Am. Crim. L. Rev. 1389 (1989).

n193. Amar, supra note 192, at 9.

n194. See, e.g., Harris v. United States, 390 U.S. 234, 236 (1968) ("It has long been settled that objects falling in the plain view of an officer who has a right to be in the position to have that view are subject to seizure and may be introduced in evidence.").

n195. See Katz v. United States, 389 U.S. 347, 347 (1967). For a discussion of the reasonable expectation of privacy test, see infra Part III.A.2.

n196. See U.S. Const. amend. IV.

n197. See Amar, supra note 192, at 3-4.

n198. See id.; Sherry F. Colb, The Qualitative Dimension of Fourth Amendment "Reasonableness," 98 Colum. L. Rev. 1642, 1648 (1998); Wasserstrom & Seidman, supra note 110, at 26-27.

n199. See Amar, supra note 192, at 16.

n200. The most famous example is Winston v. Lee, 470 U.S. 753 (1985), where the Court held that a surgical incision to remove a bullet from the suspect's body to provide evidence was unreasonable, warrant notwithstanding. However, the Court has sustained a number of other bodily intrusions to obtain evidence, such as the withdrawal of blood to test for blood alcohol level. See Schmerber v. California, 384 U.S. 757, 757 (1966).

n201. See, e.g., Colb, supra note 198, at 1645, 1687-88 (1998) (pointing out the lack of teeth in the Court's current Fourth Amendment reasonableness balancing and proposing that the Court "recognize that an "unreasonable' search in violation of the Fourth Amendment occurs whenever the intrusiveness of a search outweighs the gravity of the offense being investigated"); Tracey Maclin, Constructing Fourth Amendment Principles from the Government Perspective: Whose Amendment Is It, Anyway?, 25 Am. Crim. L. Rev. 669, 719 (1988).

n202. Brinegar v. United States, 338 U.S. 160, 175-76 (1949).

n203. Katz v. United States, 389 U.S. 347, 357 (1967).

n204. See Amar, supra note 192, at 3-4; Christopher Slobogin, The World Without a Fourth Amendment, 39 UCLA L. Rev. 1, 18 (1991).

n205. 392 U.S. 1, 1 (1968). See also Camara v. Municipal Court, 387 U.S. 523 (1967) (holding that although health, fire, and safety inspectors could not enter a home without a warrant, they need not demonstrate probable cause to obtain the warrant). For a critique of Terry and Camara, see Scott E. Sundby, A Return to Fourth Amendment Basics: Undoing the Mischief of Camara and Terry, 72 Minn. L. Rev. 383 (1988).

n206. See, e.g., Vernonia Sch. Dist. v. Acton, 515 U.S. 646 (1995) (drug testing by school officials); Nat'l Treasury Employees Union v. Von Rabb, 489 U.S. 656 (1989) (drug testing of Customs officials); Skinner v. Ry Labor Executives Ass'n, 489 U.S. 602 (1989) (drug testing of railroad employees); O'Connor v. Ortega, 480 U.S. 709 (1987) (search by government employer); New Jersey v. TLO, 469 U.S. 325 (1985) (search by school officials).

n207. Wasserstrom & Seidman, supra note 119, at 34.

n208. See Mapp v. Ohio, 367 U.S. 643, 657 (1961) (holding that the exclusionary rule applies to all government searches, state and federal).

n209. Liability under 1983 has been severely limited due to qualified immunity for police officers, see generally Harlow v. Fitzgerald, 457 U.S. 800 (1982), as well as the lack of direct liability for states. See generally Hans v. Louisiana, 134 U.S. 1 (1890). Municipalities and local governments can be sued, but they are only liable "when execution of a government's policy or custom, whether made by its lawmakers or by those whose edicts or acts may fairly represent official policy inflicts the injury." Monell v. New York City Dep't of Social Services, 436 U.S. 658, 658 (1978).

n210. 367 U.S. 643, 643 (1961).

n211. Prior to Mapp, the Court held that the exclusionary rule only applied to evidence improperly obtained by federal officials in federal court. See Weeks v. United States, 232 U.S. 383, 398 (1914). In Wolf v. Colorado, 338 U.S. 25 (1949), the Court held that the exclusionary rule does not apply to state officials. In Elkins v. United States, 364 U.S. 206 (1960), the Court began to reverse course, holding that evidence seized by state police in violation of Fourth Amendment is excluded in federal court. For more background about the development of the exclusionary rule, see Potter Stewart, The Road to Mapp v. Ohio and Beyond: The Origins, Development and Future of the Exclusionary Rule in Search and Seizure Cases, 83 Colum. L. Rev. 1365 (1983).

n212. Arnold H. Loewy, The Fourth Amendment as a Device for Protecting the Innocent, 81 Mich. L. Rev. 1229, 1266 (1983).

n213. Silverthorne Lumber Co. v. United States, 251 U.S. 385, 392 (1920).

n214. Several commentators have criticized the exclusionary rule, advocating a system of civil damages rather than the exclusion of inculpatory evidence. See Amar, supra note 192, at 28 ([the criminal defendant is] an awkward champion of the Fourth Amendment... . He is often unrepresentative of the larger class of law-abiding citizens, and his interests regularly conflict with theirs."); Id. at 20-21 (suggesting tort remedies); Christopher Slobogin, Why Liberals Should Chuck the Exclusionary Rule, 1999 U. Ill. L. Rev. 363, 400-01 (1999) (arguing for a damages remedy because the exclusionary rule fails to provide an adequate remedy to innocent people

whose Fourth Amendment rights are violated and because the rule results in judicial reluctance to expand Fourth Amendment protection). Other commentators argue that civil damages will prove to be much less successful than the exclusionary rule. See Loewy, supra note 212, at 1266 (arguing that under a damages regime, if the government really wants to search, it will conduct the illegal search and pay the damages); Maclin, supra note, 130 at 62 (contending that juries sympathize with the police in civil suits to enforce the Fourth Amendment and that damages are hard to prove).

n215. See William J. Stuntz, Privacy's Problem and the Law of Criminal Procedure, 93 Mich. L. Rev. 1016, 1019 (1995).

n216. Stuntz, supra note 119, at 442.

n217. See Stuntz, supra note 215, at 1019.

n218. Stuntz, supra note 119, at 446. See also Stuntz, supra note 215, at 1044 ("Coercion becomes the law's focus only in ... the most extreme cases. Elsewhere, the law's chief concern remains privacy").

n219. Stuntz, supra note 215, at 1077.

n220. Scott E. Sundby, "Everyman"'s Fourth Amendment: Privacy or Mutual Trust Between Government and Citizen?, 94 Colum. L. Rev. 1751, 1757-58 (1994).

n221. Id. at 1771.

n222. Id. at 1777.

n223. Id.

n224. See Solove, supra note 17, at 1146-47.

n225. See infra Part III.A.2.

n226. See infra Part III.A.2.

n227. See Aldous Huxley, Brave New World (1932); Franz Kafka, The Trial (Willa & Edwin Muir, et. al., trans., Alfred A. Knopf, Inc. 1956) (1937); Orwell, supra note 96.

n228. Raymond Shih-Ray Ku, The Founders' Privacy: The Fourth Amendment and the Power of Technological Surveillance, 86 Minn. L. Rev. 1325, 1340 (2002) (examining connection between the Fourth Amendment to separation of powers).

n229. See Daniel Yeager, Does Privacy Really Have a Problem in the Law of Criminal Procedure?, 49 Rutgers L. Rev. 1283, 1309-10 (1997) (agreeing with Stuntz that regulatory inspections can be more invasive of privacy than regular searches, but disagrees that "encounterless police investigations should be more loosely controlled so they are better aligned with regulatory inspections"). Louis Michael Seidman disputes Stuntz's view that the Fourth Amendment places privacy above coercion. See generally Louis Michael Seidman, The Problems with Privacy's Problem, 93 Mich. L. Rev. 1079 (1995).

n230. Although corporations are deemed "persons" under the Fourteenth Amendment, see Santa Clara County v. S. Pac. R.R., 118 U.S. 394, 394-95 (1886), they are not afforded Fourth Amendment rights. See California Bankers Ass'n v. Shultz, 416 U.S. 21, 65 (1974) (stating that "corporations can claim no equality with individuals in the enjoyment of a right to privacy").

n231. Stuntz, supra note 215, at 1037.

n232. Id.

n233. Amar, supra note 192, at 11.

n234. See id.

n235. Id. at 31.

n236. Levy, supra note 130, at 154.

n237. Sundby, supra note 220, at 1804.

n238. Louis Fisher, Congress and the Fourth Amendment, 21 Ga. L. Rev. 107, 115 (1986) ("The spirit and letter of the fourth amendment counseled against the belief that Congress intended to authorize a "fishing expedition' into private papers on the possibility that they might disclose a crime.").

n239. U.S. Const. amend. IV.

n240. Maclin, supra note 130, at 8. Indeed, as Maclin notes: "Everyone, including Amar, agrees that the Framers opposed general warrants." Id. at 9. See also Levy, supra note 130, at 158.

n241. Wasserstrom & Seidman, supra note 119, at 82.

n242. David M. O'Brien, Privacy, Law, and Public Policy 38 (Prager Publishers 1979). See also Levy, supra note 130, at 150; Stuntz, supra note 119, at 406.

n243. 3 The Debates in Several Conventions on the Adoption of the Federal Constitution 448-49 (Jonathan Elliot ed., 1974).

n244. James Madison, The Federalist, No. 51, in The Federalist 347, 349 (Jacob E. Cooke ed., 1961).

n245. James Madison, The Federalist, No. 48, supra note 244, at 333 (James Madison).

n246. Madison, supra note 244, at 347 (James Madison).

n247. Id. at 349.

n248. Id.

n249. Gordon S. Wood, The Creation of the American Republic 1776-1787 605 (Univ. of North Carolina Press 1969).

n250. Madison drafted the language of the Fourth Amendment. See Fisher, supra note 238, at 111-12. As Levy observes, "Madison chose the maximum protection conceivable at the time." Levy, supra note 130, at 176.

n251. Slobogin, supra note 204, at 17.

n252. William J. Stuntz, O.J. Simpson, Bill Clinton, and the Transsubstantive Fourth Amendment, 114 Harv. L. Rev. 842, 848 (2001).

n253. See id. at 848.

n254. McDonald v. United States, 335 U.S. 451, 455-56 (1948). See also Steagald v. United States, 451 U.S. 204, 212 (1981) (warrants are necessary because law enforcement officials "may lack sufficient objectivity"); Coolidge v. New Hampshire, 403 U.S. 443, 450 (1971) (stating that "prosecutors and policemen simply cannot be asked to maintain the requisite neutrality with regard to their own investigations"); Johnson v. United States, 333 U.S. 10, 13-14 (1948) (stating that the Fourth Amendment ensures that inferences of potential culpability "be drawn by a neutral and detached magistrate instead of being judged by the officer engaged in the often competitive enterprise of ferreting out crime").

n255. Amar, supra note 192, at 39.

n256. See Steiker, supra note 121, at 853.

n257. Ku, The Founders' Privacy, supra note 228, at 1333-40.

n258. 116 U.S. 616 (1886).

n259. The Fifth Amendment provides that: "No person ... shall be compelled in any criminal case to be a witness against himself ... ." U.S. Const. amend. V. The Fifth Amendment's "privilege against self-incrimination" prevents the government from compelling individuals to disclose inculpatory information about themselves. Id.

n260. See Boyd, 116 U.S. at 617-18.

n261. Id. at 630.

n262. See, e.g., Amar, supra note 192, at 22 (explaining that Boyd was part of the Lochner Court's staunch protection of property); O'Brien, supra note 242, at 22 (explaining that Boyd associated privacy with "proprietary interests"); Alan Westin, Privacy and Freedom 339-41 (1967) (describing the conception of privacy

in Boyd as "propertied privacy"); Stuntz, supra note 215, at 1030-34 (describing Boyd as part of Lochner Court's impediment to the rise of the administrative state).

n263. 96 U.S. 727 (1877).

n264. Id. at 733.

n265. 141 U.S. 250 (1891).

n266. Id. at 252.

n267. See Samuel Warren & Louis Brandeis, The Right to Privacy, 4 Harv. L. Rev. 193, 193-95 (1890).

n268. See id. at 195-97.

n269. See Irwin R. Kramer, The Birth of Privacy Law: A Century Since Warren and Brandeis, 39 Cath. U. L. Rev. 703, 704 (1990).

n270. 277 U.S. 438 (1928).

n271. Id. at 464.

n272. Id. at 473 (Brandeis, J., dissenting) (internal quotations omitted).

n273. Id.

n274. Id. at 473.

n275. 316 U.S. 129 (1942).

n276. Id.

n277. See id. at 134.

n278. 389 U.S. 347 (1967).

n279. Id. at 351-52.

n280. Id. at 361 (Harlan, J., concurring).

n281. Olmstead, 277 U.S. 438, 470 (1928) (Holmes, J., dissenting). See also Richard F. Hixson, Privacy in a Public Society: Human Rights in Conflict 49 (1987). For a history of the early days of wiretapping, see Note, The Right to Privacy in Nineteenth Century America, 94 Harv. L. Rev. 1892 (1981).

n282. Fisher, supra note 238, at 127.

n283. Id.

n284. Robert Ellis Smith, Ben Franklin's Web Site: Privacy and Curiosity from Plymouth Rock to the Internet 158 (2000).

n285. See Nardone v. United States, 302 U.S. 379 (1937) (evidence directly obtained by wiretapping excluded from evidence); Nardone v. United States, 308 U.S. 338 (1939) (evidence obtained as the fruit of illegal wiretapping could not be used in court).

n286. See Smith, supra note 284, at 160.

n287. See Diffie & Landau, supra note 128, at 155-65.

n288. See Diffie & Landau, supra note 128, at 161-62.

n289. See supra Part II.C.

n290. See supra Part II.C.

n291. See Diffie & Landau, supra note 128, at 144.

n292. Id. at 173.

n293. Samuel Dash, Richard Schwartz, & Robert Knowlton, The Eavesdroppers (1959).

n294. 488 U.S. 445 (1989).

n295. See id. at 451-52.

n296. 486 U.S. 35 (1988).

n297. Id. at 40.

n298. Id.

n299. 425 U.S. 435, 435 (1976).

n300. Id. at 444.

n301. Id. at 443.

n302. Id. at 442.

n303. 442 U.S. 735, 737 (1979).

n304. Id.

n305. Id.

n306. Id. A pen register is a device that is typically installed at the telephone company's offices that can

record the telephone numbers a person dials. A trap and trace device is a similar device that can record the telephone numbers of a person's incoming telephone traffic.

n307. Id. at 743.

n308. Id.

n309. See Orin s. Kerr, U.S. Dep't of Justice, Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations I.B.3 (Jan. 2001).

n310. Id. at I.C.1(b)(iv).

n311. 439 U.S. 128 (1978).

n312. 448 U.S. 98 (1980).

n313. Rakas, 439 U.S. at 134.

n314. Rawlings, 448 U.S. at 104-06.

n315. Miller, 425 U.S. at 443.

n316. Smith v. Maryland, 442 U.S. 735, 744 (1979).

n317. See, e.g., United States v. White, 401 U.S. 745, 750 (1971) (reasoning that the Fourth Amendment does not protect information conveyed to a government informant who wears a radio transmitter); On Lee v. United States, 343 U.S. 747, 754 (1952) (stating that the Fourth Amendment does not apply when a person misplaces her trust by talking to a bugged government informant).

n318. 385 U.S. 293 (1966).

n319. Id. at 302.

n320. Id.

n321. 385 U.S. 206 (1966).

n322. Id. at 210-11.

n323. 343 U.S. at 747.

n324. Id. at 751-52.

n325. See Solove, supra note 7, at 1435.

n326. Mary I. Coombs, Shared Privacy and the Fourth Amendment, or the Rights of Relationships, 75 Cal. L. Rev. 1593, 1594 (1987). See also Anthony G. Amsterdam, Perspectives on the Fourth Amendment, 58 Minn. L. Rev. 349, 367 (1974) (critiquing standing doctrine for viewing Fourth Amendment protections as protecting "atomistic spheres of interest of individual citizens" rather than as "regulation of governmental conduct").

n327. See, e.g., Coombs, supra note 326, at 1600 (stating that if the purpose of the exclusionary rule is deterrence, then it should apply regardless of standing); Wasserstrom & Seidman, supra note 119, at 97 (same).

n328. Rakas v. Illinois, 439 U.S. 128, 168 (1978) (White, J., dissenting).

n329. Id. at 168-69.

n330. Olmstead, 277 U.S. 438, 474 (1928) (Brandeis, J., dissenting).

n331. Id.

n332. Former 7 U.S.C. 605.

n333. Id.

n334. 302 U.S. 379 (1937).

n335. See generally Dash, Schwartz, & Knowlton, supra note 293.

n336. Wayne R. LaFave, Jerold H. Israel, & Nancy J. King, Criminal Procedure 260 (3d ed. 2000).

n337. Omnibus Crime and Control and Safe Streets Act of 1968, 18 U.S.C. 2510-22 (2001).

n338. See Regan, supra note 141, at 122-25.

n339. Wiretap Act, Electronic Communications Privacy Act, Title I, 18 U.S.C. 2510-22 (2001).

n340. Stored Communications Act, Electronic Communications Privacy Act, Title II, 18 U.S.C. 2701-11 (2000).

n341. Pen Register Act, Title III, 18 U.S.C. 3121-27 (2000).

n342. 18 U.S.C. 2510(1) (2000).

n343. 18 U.S.C. 2510(18).

n344. 18 U.S.C. 2510(2).

n345. Id. 2510(4).

n346. Id. 2510(12).

n347. See id.

n348. Id. 2518 (10)(a) (2000).

n349. See id.

n350. See id.

n351. Id. 2518.

n352. Id.

n353. Id.

n354. 18 U.S.C. 2518(5).

n355. 442 U.S. 735, 735 (1979).

n356. 425 U.S. 435, 435 (1976).

n357. This conclusion is debatable, however, because telephone companies can also store telephone communications, and it is unlikely that the Court would go so far as to say that this fact eliminates any reasonable expectation of privacy in such communications.

n358. 18 U.S.C. 2701-71.

n359. Id. 2701.

n360. 18 U.S.C. 2510(17) (emphasis added).

n361. Kerr, supra note 309, III.B.

n362. Id. at III.D.1. The government must provide prior or delayed notice to the individual. See 18 U.S.C. 2703(b)(1)(B)(i) & (b)(2).

n363. 18 U.S.C. 2703(a).

n364. Id. 2703(b).

n365. Id. 2703(d). If the government does not want to provide prior notice to the subscriber that it is seeking the information, it must obtain a warrant. Id. 2703(b). However, in a number of circumstances, notice can be delayed for up to three months after information has been obtained. Id. 2705.

n366. 18 U.S.C. 2703(c)(1)(C).

n367. Id. 2703(c)(2), amended by USA-PATRIOT Act 210.

n368. Id. 2703(c)(1)(B).

n369. Id. 2703(d).

n370. 55 F. Supp.2d 504 (W.D. Va. 1999).

n371. Id. at 506.

n372. See id. at 509.

n373. 81 F.Supp.2d 1103, 1106 (D. Kan. 2000).

n374. Id.

n375. Id.

n376. Id.

n377. Id. at 1104.

n378. Id. at 1110.

n379. See id. at 1111.

n380. 18 U.S.C. 3121(a) (1994).

n381. Id. 3123(a) (1994).

n382. "Upon application made under section 3122(a)(1), the court shall enter an ex parte order authorizing

the installation and use of a pen register or trap and trace device... ." Id. 3123 (a)(1).

n383. Id. 3123(c).

n384. Id. 3127(3), as amended by USA-PATRIOT Act 216.

n385. Id.

n386. See 29 U.S.C. 3401-22 (1994). For more information on the RFPA, see George B. Trubow & Dennis L. Hudson, The Right to Financial Privacy Act of 1978: New Protection from Federal Intrusion, 12 J. Marshall J. Prac. & Proc. 487 (1979).

n387. 29 U.S.C. 3407.

n388. Id. 3409.

n389. Id. 3408.

n390. 15 U.S.C. 1681f (2000).

n391. Id. 1681b(a)(1).

n392. 15 U.S.C. 1681u.

n393. See id.

n394. 47 U.S.C. 551 (1994).

n395. Id. 551(h)(1).

n396. Id. 551(h)(2).

n397. USA-PATRIOT Act 211.

n398. 18 U.S.C. 2710 (2001).

n399. Id. 2710(b)(2)(C).

n400. The regulations are published at 45 C.F.R. 160-64 (2001).

n401. 45 C.F.R. 164.512(f)(1)(ii) (2001).

n402. Id. 164.512(f)(2).

n403. Id. 160.102 (2001).

n404. Pew Internet & American Life Project, Institute for Healthcare Research and Policy, Georgetown

University, Exposed Online: Why the New Federal Health Privacy Regulation Doesn't offer Much Protection to Internet Users 6-8 (Nov. 2001).

n405. See id. at 7.

n406. Id. at 14, 17.

n407. 154 F. Supp. 2d 497, 497 (S.D.N.Y. 2001).

n408. See id. at 511.

n409. Fisher, supra note 238, at 152.

n410. Stuntz, supra note 252, at 857-58.

n411. Ronan E. Degnan, Obtaining Witnesses and Documents (or Things), 108 F.R.D. 223, 232 (1986).

n412. Stuntz, supra note 252, at 864.

n413. Grand juries are still used in some states as well as in the federal system. See Degnan, supra note 411, at 229.

n414. United States v. R. Enter., Inc., 498 U.S. 292, 301 (1991).

n415. Stuntz, supra note 215, at 1038.

n416. Oklahoma Press Pub. Co. v. Walling Wage, and Hour Admin., 327 U.S. 186, 208-09 (1946).

n417. Stuntz, supra note 252, at 867.

n418. 18 U.S.C. 3123(a).

n419. United States v. Fregoso, 60 F.3d 1314, 1320 (8th Cir. 1995). See also Kerr, supra note 309, IV.B.

n420. The early stages of government investigations frequently involve talking to victims, witnesses, friends, and neighbors. The police often find out about a crime when people voluntarily report suspicious activity.

n421. Julie. C. Inness, Privacy, Intimacy, and Isolation 56 (1992).

n422. Tom Gerety, Redefining Privacy, 12 Harv. C.R.-C.L. L. Rev. 233, 263 (1977). For other commentators adopting an intimacy conception of privacy, see Robert S. Gerstein, Intimacy and Privacy, in Philosophical Dimensions of Privacy: An Anthology 265 (Ferdinand David Schoeman ed. 1984), and Jeffrey H. Reiman, Privacy, Intimacy, and Personhood, in Philosophical Dimensions of Privacy: An Anthology, at 300.

n423. James Rachels, Why Privacy Is Important, in Philosophical Dimensions of Privacy: An Anthology, supra note 422, at 305-06.

n424. See Solove, supra note 17, at 1129-30.

n425. See Solove, supra note 50, at 1176-84.

n426. See Smith v. Maryland, 442 U.S. 735, 740-41 n.5 (1979) (noting that "where an individual's subjective expectations had been "conditioned' by influences alien to well-recognized Fourth Amendment freedoms, those subjective expectations obviously could play no meaningful role in ascertaining what the scope of Fourth Amendment protection was").

n427. Oath and Law of Hippocrates (circa 400 B.C.).

n428. See Current Opinions of the Judicial Council of the Amer. Med. Ass'n Canon 5.05 (1984) (observing that "the information disclosed to a physician during the course of the relationship between the physician and patient is confidential to the greatest possible degree").

n429. See, e.g., Jaffee v. Redmond, 518 U.S. 1, 6-7 (1996) (recognizing psychotherapist-patient privilege and social worker-patient privilege under the Federal Rules of Evidence); Glen Weissenberger, Federal Rule of Evidence: Rules, Legislative History, Commentary and Authority 501.8.

n430. See, e.g., Hammonds v. AETNA Casualty and Surety Co., 243 F. Supp. 793, 799 (D. Ohio 1965); Simonsen v. Swenson, 177 N.W. 831, 832 (Neb. 1920). Courts, however, have made exceptions in circumstances where disclosures must be made to protect the public. Simonsen, 177 N.W. at 832. They have even imposed tort liability when physicians or psychotherapists fail to disclose data that could lead to imminent harm. Tarasoff v. Regents of the Univ. of Cal., 551 P.2d 334, 353 (Cal. 1976).

n431. See, e.g., Cal. Health & Safety Code 199.21 (prohibiting disclosure of HIV test results); N.Y. Pub. Health L. 17 (prohibiting disclosure of minors' medical records pertaining to sexually transmitted diseases and abortion).

n432. See Upjohn Co. v. United States, 449 U.S. 383, 389 (1981).

n433. See Weissenberger, supra note 429, at 190.

n434. See id.

n435. Jaffee, 518 U.S. at 15.

n436. Christopher Slobogin, Technologically-Assisted Physical Surveillance: The American Bar Association's Tentative Draft Standards, 10 Harv. J.L. & Tech. 383, 400 (1997).

n437. 5 U.S.C. 552(a)(5) (2000).

n438. Amsterdam, supra note 326, at 404.

n439. See supra Part II.B.

n440. Solove, supra note 7, at 1427-28.

n441. Edward J. Janger & Paul M. Schwartz, The Gramm-Leach-Bliley Act, Information Privacy, and the Limits of Default Rules, 86 Minn. L. Rev. 1219, 1241-42 (2002).

n442. Schwartz, Internet Privacy and the State, supra note 6, at 822-23.

n443. U.S. Const. amend V.

n444. Ruth Marcus, To Some in the Law, Starr's Tactics Show a Lack of Restraint, Wash. Post, Feb. 13,

1998, at A1.

n445. Trammel v. United States, 445 U.S. 40, 49-50 (1980). However, a spouse can waive the right to refuse to testify, and, if so, the defendant spouse cannot prevent his or her spouse from testifying. Id. at 52-53.

n446. In re Grand Jury, 103 F.3d 1140, 1146 (3d Cir. 1997) (observing that most federal and state courts have rejected the privilege).

n447. Pearse v. Pearse, 63 Eng. Rep. 950, 957 (1846).

n448. United States v. Neal, 532 F. Supp. 942, 946 (D. Colo. 1982).

n449. 116 U.S. 616 (1886).

n450. See id. at 638.

n451. 255 U.S. 298 (1921).

n452. Id. at 309.

n453. 387 U.S. 294 (1967).

n454. See id. at 309-10.

n455. 335 U.S. 1 (1948).

n456. 409 U.S. 322 (1973).

n457. See id. at 323.

n458. See id.

n459. Id. at 328.

n460. Id. at 329.

n461. 425 U.S. 391 (1976).

n462. See id. at 414.

n463. Id. at 401 (internal quotations and alterations omitted).

n464. Id.

n465. Stuntz, supra note 215, at 1050.

n466. Fisher, supra note 238, at 151.

n467. 436 U.S. 547 (1978).

n468. Id. at 571.

n469. Pub. L. No. 96-440, 94 Stat. 1879, codified at 42 U.S.C. 2000aa (1994).

n470. Some states, such as California, have enacted laws requiring the notification of the people to whom the records pertain. See Cal. Code Civ. Proc. 1985.3; Degnan, supra note 411, at 233.

n471. See supra Part IV.B.

n472. I am not contending that all of the existing exceptions to notice are valid; rather, I believe that some of these exceptions are acceptable.

n473. 140 F. Supp.2d 1088 (W.D. Wash. 2001).

n474. Id. at 1089-93.

n475. See, e.g., Columbia Ins. Co. v. Seescandy.com, 185 F.R.D. 573 (N.D. Cal. 1999).

n476. Stuntz, supra note 252, at 857.

n477. Steiker, supra note 121, at 834.

n478. 5 U.S.C. 552a (2000).

n479. See, e.g., Schwartz, supra note 5, at 585-86.

n480. Gellman, supra note 141, at 198.

n481. Solove, supra note 50.

TAB 15

1 of 1 DOCUMENT

New York University Law Review

April, 2007

82 N.Y.U.L. Rev. 112

LENGTH: 32043 words

ARTICLE: THE FIRST AMENDMENT AS CRIMINAL PROCEDURE

NAME: Daniel J. Solove *

BIO: * Copyright © 2007 by Daniel J. Solove. Associate Professor, George Washington University Law School; J.D., Yale Law School. For helpful comments, thanks to Jack Balkin, Paul Butler, Morgan Cloud, Anuj Desai, Thomas Dienes, David Fontana, Marcia Hofmann, Chris Hoofnagle, Orin Kerr, Chip Lupu, Robert Post, Peter Raven-Hansen, Neil Richards, Fred Schauer, Paul Schwartz, Chris Slobogin, Charlie Sullivan, Michael Sullivan, Andrew Taslitz, Robert Tsai, Robert Tuttle, and Eugene Volokh. I would also like to thank Judith Krug, who helped me track down cases involving subpoenas and requests for library records. The Criminal Law Professors Workshop held at the George Washington University Law School yielded very helpful comments. My research assistants James Murphy, Tiffany Stedman, and Sava Savov provided excellent research support.

SUMMARY:
... This Article explores the relationship between the First Amendment and criminal procedure. ... Although government information gathering can implicate central First Amendment values, it has typically been regulated by criminal procedure rules established under the Fourth and Fifth Amendments. ... Under the Federal Rules of Criminal Procedure, a "subpoena may order the witness to produce any books, papers, documents, data, or other objects the subpoena designates. ... Although the First Amendment itself has seldom been applied in the context of a search, seizure, or other government investigation, the Supreme Court has on rare occasion considered how First Amendment values affect traditional Fourth Amendment cases. ... One approach would be to conclude that the First Amendment is implicated only when government information gathering falls within the Fourth Amendment's scope. ... Stuntz contends that the law of search and seizure is the "consequence of the strong tradition of using Fourth and Fifth Amendment law as a shield against government information gathering - a tradition that has more to do with protecting free speech than with regulating the police. ... The chilling effect doctrine recognizes that the First Amendment can be implicated indirectly and not just through direct legal prohibitions on speech. ...

HIGHLIGHT:

This Article explores the relationship between the First Amendment and criminal procedure. These two domains of constitutional law have long existed as separate worlds, rarely interacting with each other despite the fact that many instances of government information gathering can implicate First Amendment freedoms of speech, association, and religion. The Fourth and Fifth Amendments used to provide considerable protection for First Amendment interests, as in the famous 1886 case Boyd v. United States, in which the Supreme Court held that the government was prohibited from seizing a person's private papers. Over time, however, Fourth and Fifth Amendment protection has shifted, and countless searches and seizures involving people's private papers, the books they read, the websites they surf, and the pen names they use when writing anonymously now fall completely outside the protection of constitutional criminal procedure. Professor Solove argues that the First Amendment should protect against government information gathering

that implicates First Amendment interests. He contends that there are doctrinal, historical, and normative justifications for developing what he calls "First Amendment criminal procedure." Solove sets forth an approach for determining when certain instances of government information gathering fall within the regulatory domain of the First Amendment and what level of protection the First Amendment should provide.

TEXT:
[*113]

Introduction

Suppose the government is interested in finding out about your political beliefs, religion, reading habits, or the things you write and say to others. To uncover this information, law enforcement officials construct a bibliography of the books you read using records at bookstores and libraries. They assemble a list of people with whom you communicate using records obtained from your Internet Service Provider (ISP) and phone company. They seize your diary and personal writings. To what extent do the Fourth and Fifth Amendments restrict the government's investigation?

In many instances, not at all. A century ago, the Fourth and Fifth Amendments would have significantly restricted government information **[*114]** gathering that involves what I will refer to as "First Amendment activities" - speech, association, consumption of ideas, political activity, religion, and journalism. n1 But today, the Fourth and Fifth Amendments play a much diminished role in these contexts. First, the Supreme Court has held that the use of a subpoena to obtain documents and testimony receives little, if any, Fourth or Fifth Amendment protection. n2 Subpoenas are orders compelling the production of documents or information. They are issued without judicial approval, and they have few limitations beyond a requirement that the information be relevant to an investigation. n3 As a result, the government can readily use subpoenas to gather information pertaining to communications, writings, and the consumption of ideas. Second, the Court has held that the Fourth Amendment does not cover instances when a person's information is gathered from third parties. n4 In the Information Age, a massive amount of data about our lives - data that may pertain to First Amendment activities - is maintained by third-party businesses and organizations.

Does the First Amendment provide any protection? At first blush, the question seems odd. The rules that regulate government investigations have typically emerged from the Fourth and Fifth Amendments, not the First. Lawyers and judges generally do not think of the First Amendment as having much relevance to criminal procedure, let alone as providing its own criminal procedure rules. The First Amendment is usually taught separately from the Fourth and Fifth Amendments, and judicial decisions on criminal procedure only occasionally mention the First Amendment. I contend in this Article, however, that the First Amendment must be considered alongside the Fourth and Fifth Amendments as a source of criminal procedure.

First Amendment activities are implicated by a wide array of law enforcement data-gathering activities. Government information gathering about computer and Internet use, for example, can intrude on a **[*115]** significant amount of First Amendment activity. Searching or seizing a computer can reveal personal and political writings. Obtaining e-mail can provide extensive information about correspondence and associations. Similarly, ISP records often contain information about speech, as they can link people to their anonymous communications. AOL, for example, receives about a thousand requests per month for use of its customer records in criminal cases. n5

The government can also use subpoenas to gather information about First Amendment activities such as book reading and personal writing. Indeed, the FBI once subpoenaed six years of customer records from Arundel Books, an alternative book retailer, in connection with an investigation of political campaign contributions. n6 Independent Counsel Kenneth Starr subpoenaed records of Kramerbooks & Afterwords, a bookstore in Washington, D.C., regarding books Monica Lewinsky purchased for President Bill Clinton. n7 The government has also subpoenaed people's

writings, documents, and even their diaries. The Senate Ethics Committee, for example, subpoenaed the diaries of Republican Senator Bob Packwood as part of its investigation of sexual harassment charges against the senator. n8

Government information gathering can also implicate other First Amendment protections, such as freedom of association and freedom of the press. Freedom of association can be implicated when the government monitors or attempts to infiltrate political groups. Freedom of the press can be compromised when the government subpoenas journalists to provide the identities of confidential sources, or when the police search the offices or computers of media entities. And with blogs supplementing the traditional media, searches of individual homes and computers might also implicate journalistic activities. n9

Today, in an effort to fight the war on terrorism and protect national security, the government gathers extensive information about people's associational ties and their communicative activity. Section 215 of the USA PATRIOT Act permits the FBI to "make an application for an order requiring the production of any tangible things (including books, records, papers, documents, and other items) for an **[*116]** investigation ... to protect against international terrorism or clandestine intelligence activities." n10 Shortly after September 11th, the Bush Administration authorized the National Security Agency (NSA) to engage in warrantless wiretapping of international phone calls and the gathering of phone records en masse. n11 The FBI began canvassing for information about worshippers at several mosques. n12 Furthermore, the government has been engaging in "data mining" - examining data for various links between people or for certain patterns of behavior. n13

Although First Amendment activities are frequently involved in government investigations, the First Amendment is rarely invoked when courts apply the constitutional procedural safeguards that govern such investigations. n14 This Article endeavors to establish a foundation for the development of First Amendment criminal procedure. I contend that there are doctrinal, historical, and normative foundations for the First Amendment to play a significant role in regulating government information gathering. I explore when government investigations should trigger First Amendment protection and what kinds of safeguards the First Amendment should require.

Part I discusses the current landscape of criminal procedure protections for First Amendment activity and argues that current rules leave many activities that are central to First Amendment values unprotected. Government information gathering frequently implicates First Amendment values, but courts and commentators analyzing the constitutionality of government searches have traditionally focused only on the Fourth and Fifth Amendments. Under current law, however, much government information gathering affecting First **[*117]** Amendment activity falls outside the scope of Fourth and Fifth Amendment regulation.

Part II sets forth the positive case for First Amendment criminal procedure. I contend that First Amendment protection against government information gathering is justified by the historical connections between the First, Fourth, and Fifth Amendments, the history of government investigations into First Amendment activity, and several lines of First Amendment doctrine.

Part III explores the contours and consequences of developing First Amendment criminal procedure. The First Amendment could conceivably be applied so broadly that it would swallow up the field of criminal procedure. I discuss where the boundaries of First Amendment protection should extend and the kind of protection the First Amendment should require. I then apply my theory of First Amendment criminal procedure to various examples of government information gathering.

I

Criminal Procedure and First Amendment Activities

Although government information gathering can implicate central First Amendment values, it has typically been regulated by criminal procedure rules established under the Fourth and Fifth Amendments. I argue that current criminal

procedure rules underprotect First Amendment activities, leaving them exposed to intrusive government information gathering. While courts have acknowledged that searches for certain materials may implicate First Amendment values, the Supreme Court has not resolved the question of how to protect First Amendment activities when they fall outside the scope of the Fourth Amendment. I argue that the First Amendment itself must be understood as an independent source of criminal procedure rules.

A. Two Separate Worlds of Constitutional Law

Constitutional criminal procedure and the First Amendment currently occupy two worlds that rarely intermingle. In law schools, the First Amendment is taught separately from the Fourth and Fifth Amendments. First Amendment scholars rarely delve into constitutional criminal procedure, and criminal procedure scholars rarely consider the First Amendment implications of government searches. This is not surprising, given that the criminal procedure amendments and the First Amendment operate to protect constitutional rights in very different ways. The Fourth and Fifth Amendments establish procedures **[*118]** for government information gathering - thresholds to justify searches, requirements for judicial oversight, rules to minimize the scope of searches, and limits on interrogation. The First Amendment, in contrast, works primarily by striking down the application of particular laws, regulations, or executive activities.

In examining a challenge to a government activity under the Fourth Amendment, n15 a court must first determine whether the government action falls within the scope of the Amendment's protection, and only then ask whether appropriate procedures were followed. To determine whether a particular information gathering practice falls within the scope of the Fourth Amendment, courts apply the "reasonable expectation of privacy" test set forth in Justice Harlan's concurrence in Katz v. United States. n16 The test examines whether a person exhibits an "actual (subjective) expectation of privacy" and whether "the expectation [is] one that society is prepared to recognize as 'reasonable.'" n17

If the Fourth Amendment applies, it requires that a search or seizure be "reasonable." In most cases, a search will be reasonable if government officials have obtained a search warrant, which requires establishing "probable cause" before a neutral judge or magistrate. n18 Probable cause requires "reasonably trustworthy information ... sufficient... to warrant a man of reasonable caution in the belief that an offense has been or is being committed" or that evidence will be found in the place to be searched. n19 When the Fourth Amendment is violated, the typical remedy is the "exclusionary rule" - the evidence obtained through the violation is suppressed at trial. n20

The Fifth Amendment regulates government interrogations meant to glean incriminating information. The Fifth Amendment's privilege against self-incrimination provides: "No person shall ... be compelled in any criminal case to be a witness against himself." n21 As interpreted by the Supreme Court, the privilege bars compelled testimonial **[*119]** self-incrimination. n22 If a defendant's statement is obtained in violation of the Fifth Amendment, it cannot be used at trial. n23

In contrast, a court hearing a First Amendment challenge to a law generally examines the law's substantive validity. The First Amendment restricts laws "respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances." n24 Most restrictions on freedom of speech or association are analyzed under either strict or intermediate scrutiny, depending on the nature of the restriction. Under strict scrutiny, a law must be the "least restrictive means" to achieve a "compelling" government interest, n25 while intermediate scrutiny requires a law to be "narrowly tailored" to a "significant government interest" and "leave open ample alternative channels of communication." n26 Laws and actions that do not survive the appropriate level of scrutiny are invalid.

Thus, under current doctrine, the Fourth and Fifth Amendments mandate procedures for investigating violations of law, while the First Amendment is largely about the validity of substantive laws. First Amendment doctrine tells us a lot about what conduct can or cannot be criminalized, but it tells us little about what process the government must follow to conduct investigations. As a result, when government information gathering implicates First Amendment activities, it is

regulated, if at all, only by the Fourth and Fifth Amendments. But as I demonstrate below, Fourth and Fifth Amendment doctrine is inadequate to safeguard central First Amendment values that are implicated by government information gathering.

B. First Amendment Values and Government Information Gathering

Today in the United States, few question the importance of the First Amendment. Perhaps more than any other constitutional amendment, the First Amendment has iconic status and wields tremendous **[*120]** power. n27 It covers a broad constellation of fundamental freedoms, encompassing speech, association, the consumption of ideas, the press, and religion. As John Milton eloquently argued in 1644, "the liberty to know, to utter, and to argue freely according to conscience [is] above all liberties." n28 First Amendment freedoms promote individual autonomy n29 and are essential for democracy. n30 As Justice Brandeis argued, "freedom to think as you will and to speak as you think are means indispensable to the discovery and spread of political truth," and "without free speech and assembly discussion would be futile." n31 The Supreme Court once observed that the First Amendment is "the matrix, the indispensable condition, of nearly every other form of freedom." n32

Understood broadly, the First Amendment aims to ensure freedom of thought and belief. The Court clearly articulated this value in West Virginia Board of Education v. Barnette n33 when it invalidated a compulsory flag salute because it invaded "the [individual's] sphere of intellect and spirit." n34 Vincent Blasi and Seana Shiffrin have noted that "what underpins Barnette is the First Amendment interest in the speaker's freedom of thought and freedom of conscience." n35 Further, they observe: "The speaker, as well as the community of which she is a part, has an interest in her thinking and reasoning about **[*121]** subjects sincerely and authentically." n36 Democracy depends upon citizens who are free to formulate their own beliefs. n37 Government information gathering can threaten the ability to express oneself, communicate with others, explore new ideas, and join political groups.

Government probing can lessen the effectiveness of democratic participation by depriving speakers of anonymity, which can be essential for forthright expression. The Supreme Court has held that protecting anonymity is necessary to foster speech about unpopular views: "Persecuted groups and sects from time to time throughout history have been able to criticize oppressive practices and laws either anonymously or not at all." n38 According to the Court, "identification and fear of reprisal might deter perfectly peaceful discussions of public matters of importance." n39 Sociologist Robert Putnam points out that "anonymity and the absence of social cues inhibit social control - that is, after all, why we have the secret ballot." n40 Investigative inquiries into the identities of speakers can thus deter them from uttering their views or dilute the vitality of their speech.

Government information gathering can also discourage or subdue conversations. Traditionally, the First Amendment was understood as protecting the speaker at the street corner or the political group staging a public demonstration. Alexander Meiklejohn's vision of free speech exemplifies this view; he uses the analogy of the town meeting as the epitome of what the First Amendment protects. n41 But political discourse does not just occur on soapboxes before large crowds; it also thrives in private enclaves between small groups of people. Freedom of speech should and does protect the ability of individuals to communicate with each other, regardless of whether the exchange of ideas occurs between two people or among a million. In other words, the First Amendment safeguards not just speeches and rallies but conversations. People formulate their political opinions and debate politics mostly off-stage, between friends, family, and acquaintances, among **[*122]** fellow religious worshippers, and within groups with shared values and commitments. Such conversations depend upon privacy. Without protection against government probing, countless conversations might never occur or might be carried on in more muted and cautious tones.

In addition to protecting expression, the First Amendment safeguards the receipt of ideas. n42 Reading, listening, and engaging in intellectual inquiry facilitate the formulation of the thoughts and beliefs from which speech germinates. n43 Even when not leading to speech, the right to receive ideas is still valuable, for as Marc Blitz contends, it promotes "vigorous self-examination and free intellectual exploration." n44 "When individuals encounter dissenting or obscure views merely by receiving or exploring information," Blitz argues, "they exercise their First Amendment freedom

without saying a word about what they believe." n45 The receipt of ideas is essential for furthering not just individual autonomy, but also democratic participation. Exposure to ideas shapes people's political beliefs even if they are never publicly expressed. People might vote differently, for example, after encountering new ideas. Government information gathering of the consumption of ideas can make people reticent to read controversial books or probe unpopular viewpoints. People might be fearful of being linked to ideas they merely want to investigate rather than adopt or endorse.

As with the communication and receipt of ideas, freedom of association can be quelled by governmental invasions of privacy. Free association is fundamental to democratic participation; in the words of Alexis de Tocqueville, it is one of the "foundations of society." n46 People may be reluctant to join certain groups if the government is recording membership information. As the Supreme Court once declared: "Inviolability of privacy in group association may in many circumstances be indispensable to preservation of freedom of association, particularly where a group espouses dissident beliefs." n47

[*123] Therefore, uninhibited conversations, association, and exchange of ideas can be stifled by the searching light of government inquest and observation. Surveillance can make people reluctant to engage in robust and candid discourse. n48 It can inhibit deliberative democracy and individual self-determination. n49 Government information gathering can thus strike at the heart of First Amendment values.

C. Criminal Procedure and First Amendment Values

Although government information gathering often implicates First Amendment values, courts and commentators have generally analyzed information gathering under the Fourth and Fifth Amendments, leaving First Amendment activities with little protection. In many cases, Fourth and Fifth Amendment protection has receded in precisely those areas most important to First Amendment values.

The ability to keep personal papers and records of associational ties private is a central First Amendment value. But despite their First Amendment importance, the broad subpoena power and the Fourth Amendment's third-party doctrine leave these documents unprotected from government scrutiny. If the government wants to search a person's home for documents, the Fourth Amendment will usually require a search warrant supported by probable cause. n50 However, if the government uses a subpoena, the level of Fourth and Fifth Amendment protection is different. Under the Federal Rules of Criminal Procedure, a "subpoena may order the witness to produce any books, papers, documents, data, or other objects the subpoena designates." n51 Subpoenas do not require probable cause or even judicial supervision. n52 Although subpoenas may be challenged in court, **[*124]** they usually are quashed only if they severely overreach. n53 As William Stuntz notes, Kenneth Starr in his investigation of President Clinton used subpoenas much more than search warrants:

This use of the grand jury and its power to subpoena, rather than the police and their power to search, gave Starr's team the authority to find out just about anything it might have wanted. For while searches typically require probable cause or reasonable suspicion and sometimes require a warrant, subpoenas require nothing, save that the subpoena not be unreasonably burdensome to its target. Few burdens are deemed unreasonable. n54

The Fourth and Fifth Amendments provide only minimal limitations on subpoenas. In United States v. Dionisio, n55 the Supreme Court held that subpoenas generally do not constitute a Fourth Amendment search. n56 The Fifth Amendment will also not generally bar subpoenas for a person's documents even when they contain incriminating statements; instead, it will only provide protection when the act of producing documents "has communicative aspects of its own, wholly aside from the contents of the papers produced." n57 As Christopher Slobogin observes, however, the

"lion's share of subpoenas that seek personal papers ... are directed at third parties." n58 The Court concluded in Couch v. United States n59 and in Fisher v. United States n60 that **[*125]** subpoenas to third parties for a person's papers do not implicate the Fifth Amendment.

Likewise, the Fourth Amendment does not provide protection when the government seeks information about a person from a third party, whether through a subpoena or through some other means. Under the third-party doctrine, if a person's information is maintained by a third party, then she has no reasonable expectation of privacy in that information. In United States v. Miller, n61 the Supreme Court concluded that there is no reasonable expectation of privacy in financial records maintained by one's bank: "The Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities." n62 The Court held in Smith v. Maryland n63 that people cannot "harbor any general expectation that the [phone] numbers they dial will remain secret" because they "know that they must convey numerical information to the phone company." n64 Thus, the government could access the phone numbers dialed (via a pen register) without implicating the Fourth Amendment. n65

In several cases, lower courts have also applied the third-party doctrine to records held by ISPs of a person's communications via computer. In United States v. Hambrick, n66 the government obtained a defendant's customer records from his ISP, MindSpring. With these records, law enforcement officials were able to link his pseudonymous pen name to his real name. The court concluded that the defendant had no Fourth Amendment protection in his records because he "knowingly revealed his name, address, credit card number, and telephone number to MindSpring and its employees." n67 Likewise, in United States v. Kennedy, n68 the court concluded that a defendant's ISP records were not protected by the Fourth Amendment because he "knowingly revealed [to his ISP] all information connected to [his] IP address." n69 In Guest v. Leis, n70 the Sixth Circuit held that individuals "lack a Fourth Amendment privacy interest in their [Internet service] **[*126]** subscriber information because they communicate[] it to the systems operators." n71

Therefore, if one's papers are confined to one's home, they are protected by the general rule that the government needs a warrant to search one's home. But if one's papers (or the data contained within them) are in the hands of another, they enjoy little or no Fourth and Fifth Amendment protection. As I have discussed extensively elsewhere, much of our personal information today is in the hands of third parties, n72 and much of this information concerns activities protected under the First Amendment.

The third-party doctrine reflects a broader principle about how the Fourth Amendment operates. The Fourth Amendment focuses not on what various records or documents can reveal, but rather upon where they are located or who possesses them. For example, bags and containers are protected from searches under the Fourth Amendment, but garbage is not. n73 As the Court observed in another case, "Once placed within ... a container, a diary and a dishpan are equally protected by the Fourth Amendment." n74

Due to changes in technology and the realities of modern life, much First Amendment activity now leaves digital fingerprints beyond private zones protected by the Fourth Amendment. In the past, personal papers and correspondence were often located in people's homes, which have always received strong Fourth Amendment protection. People's conversations would take place in private places or through sealed letters, often shielding them from government access without a search warrant. Today, however, Internet surfing in the seclusion of one's own home creates data trails with third parties in distant locations. The books a person buys can be tracked by looking at records maintained by booksellers such as Amazon.com. Much of what a person says and does today finds its way into the record systems of various companies. In the past, much speaking, association, and reading occurred in secluded places, walled off from the rest of the world. But with modern technology, First Amendment activity **[*127]** occurs via e-mail, the Internet, and the telephone. It is no longer confined to private zones such as the home and no longer benefits from Fourth Amendment protection.

The ability to engage in political activity and discussion in public is also of central importance to the First Amendment, but falls outside Fourth Amendment protection. Merely observing something in "plain view" is not a search. n75 For example, the government may monitor various political groups or may send officers to record

information about public demonstrations. The Court has held that the Fourth Amendment does not apply to surveillance in public. n76

In addition, government officials may use informants or pose as secret agents to infiltrate a political group. Under the "assumption of risk" doctrine in Fourth Amendment law, information is not protected if a person revealed it to a police informant or undercover officer. n77 In Hoffa v. United States, n78 for example, the Court concluded that there was no Fourth Amendment protection when a defendant made statements to an undercover informant because the informant was "not a surreptitious eavesdropper." n79 The defendant willingly spoke with the informant and relied "upon his misplaced confidence that [the informant] would not reveal his wrongdoing." n80 Informants or undercover agents can even use concealed electronic surveillance devices without triggering Fourth Amendment protection. n81

Thus through a combination of the Court's interpretive maneuverings and technological change, the Fourth and Fifth Amendments have receded from protecting against many instances of law enforcement activity that implicate First Amendment values. When the Fourth and Fifth Amendments protected these activities, First Amendment protection may have been redundant and unnecessary. Although the Fourth and Fifth Amendments have receded from this **[*128]** area, First Amendment protection should remain. Since the Fourth and Fifth Amendments are increasingly not applicable, it is even more imperative that the First Amendment safeguard activities central to its values and purpose.

D. An Open Question

Although the First Amendment itself has seldom been applied in the context of a search, seizure, or other government investigation, n82 the Supreme Court has on rare occasion considered how First Amendment values affect traditional Fourth Amendment cases. In one line of cases, the Supreme Court recognized the relationship between the First and Fourth Amendments in searches and seizures of expressive material. These cases hold that when First Amendment activities are implicated by a search or a seizure, Fourth Amendment procedures must be followed with "scrupulous exactitude." But despite the rigorous-sounding language, the "scrupulous exactitude" standard merely requires following the typical protections of the Fourth Amendment (i.e., warrants supported by probable cause). More importantly, the scrupulous exactitude cases tell us nothing about what procedures should apply when First Amendment activity falls outside the scope of current Fourth and Fifth Amendment protection.

The scrupulous exactitude cases began in 1961 when the Supreme Court held in Marcus v. Search Warrant n83 that large-scale searches and seizures of obscene publications provided too much discretion to police officers to determine which materials to seize. n84 The Court concluded that these searches and seizures were unconstitutional, noting that "historically the struggle for freedom of speech and press in England was bound up with the issue of the scope of the search and seizure power." n85 A few years later, a plurality of Justices explained in A Quantity of Books v. Kansas n86 that because obscene books **[*129]** enjoyed First Amendment protection, they could not be treated like any other form of contraband. n87

In later cases, the Court went on to find that First Amendment rights could be sufficiently protected by means of usual Fourth Amendment procedures. Stanford v. Texas n88 concerned an investigation by Texas authorities into John Stanford's involvement with the Communist Party. Pursuant to a warrant, Texas police searched Stanford's home to gather evidence that he had violated a Texas statute outlawing the Communist Party. n89 The police hauled away fourteen cartons consisting of about two thousand books and papers, including works by Karl Marx, Jean-Paul Sartre, Fidel Castro, Pope John XXIII, and, ironically, Justice Hugo Black. Stanford's records, bills, and personal correspondence were also seized. The Supreme Court held first that the seizure violated the Fourth Amendment because it took place pursuant to a "general warrant," the "kind which it was the purpose of the Fourth Amendment to forbid." n90 The Court then noted that the search also implicated First Amendment rights, which could be adequately protected only by careful adherence to the requirements of the Fourth Amendment:

In short ... the constitutional requirement that warrants must particularly describe the "things to be seized" is to be accorded the most scrupulous exactitude when the "things" are books and the basis for their seizure is the ideas which they contain. No less a standard could be faithful to First Amendment freedoms. n91

In at least one case, Roaden v. Kentucky, n92 the Court suggested that the First Amendment might expand the scope of the Fourth Amendment, while not necessarily expanding the type of protections required. Roaden involved a sheriff who watched a film at a drive-in theater, concluded it was obscene, arrested the manager, and seized a copy of the film without a warrant. The Court found that the seizure implicated the First Amendment right to free speech, and suggested that the First Amendment implications provided a basis for Fourth Amendment protection: "The setting of the bookstore or the commercial theater, each presumptively under the protection of the First **[*130]** Amendment, invokes such Fourth Amendment warrant requirements because we examine what is 'unreasonable' in the light of the values of freedom of expression." n93

A 1978 case illustrated that Fourth Amendment "scrupulous exactitude" protection of First Amendment activity will in most
cases only require a warrant supported by probable cause. Zurcher v. Stanford Daily involved a police search of a college newspaper's office to gather photographs of a demonstration that had turned violent. n94 Although the newspaper did not participate in the demonstration and nobody at the newspaper was suspected of criminal activity, the Fourth Amendment only required that the police obtain a warrant by demonstrating probable cause that the search would uncover evidence of a crime. n95 The newspaper argued that search of its offices implicated the First Amendment because it "seriously threatened the ability of the press to gather, analyze, and disseminate news." n96

Although the Court recognized that First Amendment activities were implicated by the search, it concluded that "the prior cases do no more than insist that the courts apply the warrant requirements with particular exactitude when First Amendment interests would be endangered by the search." n97 Accordingly, First Amendment interests are sufficiently protected by "the preconditions for a warrant." n98 In later cases, the Court clarified that the First Amendment does not require a "higher standard" than a warrant supported by probable cause for seizures of books or films. n99 So while the Court has recognized that government information gathering implicates First Amendment rights, it has found that these rights are not deserving of more criminal procedure protections than other activities.

In these cases, however, the Court left a key question unanswered. In each case where the Court found that First Amendment **[*131]** rights were compromised, the government information gathering fell within the ambit of the Fourth Amendment. But when the Fourth Amendment does not apply, there are no procedures to follow with scrupulous exactitude. If government information gathering implicates First Amendment activities but the Fourth Amendment does not apply, what protections should be required?

One approach would be to conclude that the First Amendment is implicated only when government information gathering falls within the Fourth Amendment's scope. However, although they overlap to some degree, the First and the Fourth Amendments protect different things. The Fourth Amendment is currently understood by the Court to protect privacy, and the test for determining the scope of the Fourth Amendment is the existence of a reasonable expectation of privacy. n100 First Amendment activity, in contrast, can be hindered without a violation of privacy, such as when the government engages in public surveillance of political activity. If First Amendment activities are implicated, it is not clear why protection should depend upon whether the activities are also encompassed within the scope of the Fourth Amendment.

Another approach is to conclude that the First Amendment enlarges the scope of the Fourth Amendment. The Court could draw on Roaden v. Kentucky and the scrupulous exactitude cases to conclude that the scope of the Fourth Amendment must be determined not only by reference to the reasonable expectation of privacy test but also based on the extent to which First Amendment activities are implicated. Akhil Amar, for example, has argued that First

Amendment activities should be a factor in assessing the reasonableness of a search. According to Amar, reasonableness is a way of "integrating First Amendment concerns explicitly into the Fourth Amendment analysis," n101 because, as the Court itself has noted, "A seizure reasonable as to one type of material in one setting may be unreasonable in a different setting or with respect to another kind of material." n102 Integrating First Amendment values into Fourth Amendment analysis certainly might protect some First Amendment activities involved in government information gathering. But the substantive values underpinning the First Amendment are more thoroughly developed in First **[*132]** Amendment jurisprudence, and it is more appropriate to look to that jurisprudence for guidance.

In this Article, I argue that the First Amendment should and does provide an independent basis for protection from intrusive government information gathering. The scrupulous exactitude cases hold that where both the First and the Fourth Amendment are applicable, the procedures of the Fourth are sufficient to satisfy the demands of the First. But when those Fourth Amendment procedures are unavailable because the Court has concluded that the Fourth Amendment does not cover a particular activity, the scrupulous exactitude cases do not tell us what to do. If the government information gathering still implicates First Amendment rights, the First Amendment should require its own procedural safeguards. Under this approach, the First Amendment serves as an independent source of criminal procedure.

II

First Amendment Criminal Procedure

In this Part, I set forth the historical and doctrinal basis for developing the First Amendment as an independent source of criminal procedure. While courts have not traditionally looked to the First Amendment as an independent source of procedural rules, important strands of history and doctrine justify First Amendment protections in the information gathering context. First, the amendments in the Bill of Rights need not be compartmentalized to isolated and separate domains. The First, Fourth, and Fifth Amendments share a common history. Among the factors that motivated the adoption of these amendments were government inquests into speech, religion, belief, and association. More recent history also shows that our Founders' concerns about these inquests are still relevant. Second, current First Amendment doctrine on surveillance of political activities, anonymity, free association, press protection, and subpoenas provides a foundation for the development of First Amendment criminal procedure.

A. Historical Justifications

1. The Origins of the First, Fourth, and Fifth Amendments

An examination of the historical ties between the First, Fourth, and Fifth Amendments demonstrates the significant extent to which First Amendment values are implicated in criminal procedure. n103 **[*133]** Contemporary constitutional pedagogy has often splintered the Bill of Rights into separate domains, but as Akhil Amar argues, "our Constitution is a single document ... not a jumble of disconnected clauses." n104 "Instead of being studied holistically," Amar observes, "the Bill [of Rights] has been chopped up into discrete chunks of text, with each bit examined in isolation." n105 This is especially true with the First Amendment and the Fourth and Fifth Amendments, which are often taught separately in different courses. But while the First, Fourth, and Fifth Amendments are often studied separately, they in fact emerged to protect related values.

The First, Fourth, and Fifth Amendments share a common background in concerns about seditious libel. n106 As William Stuntz observes: "Fourth and Fifth Amendment history ... has more in common with the First Amendment ... than with criminal procedure as we know it today." n107 Prosecutions for seditious libel were frequently used in Britain in the eighteenth century as a device to suppress criticism of the government, and there were well over a thousand seditious speech prosecutions in the colonies. n108

The Framers were influenced by a series of high-profile seditious libel cases that took place both in the colonies and in England. n109 In particular, John Peter Zenger was tried for seditious libel in 1735 in colonial New York, and a jury nullified the law to acquit him. n110 The **[*134]** Zenger case, in the words of one commentator, served "as a crucible for the flames of liberty and freedom of the press that were stirring in the Colonies." n111

An English case, Wilkes v. Wood, n112 also generated an enormous buzz in the colonies. In 1763 in England, John Wilkes, a prominent member of Parliament, published a series of anonymous pamphlets titled The North Briton, including an issue Number 45 that sharply criticized the King. n113 Pursuant to a general warrant authorizing a search for anything connected to The North Briton Number 45, government officials searched Wilkes's home, seized his papers, and arrested him. n114 The warrant did not mention Wilkes by name. Such general warrants were common at the time and were used to muzzle the press and squelch political dissent. n115

Wilkes and others initiated a civil trespass lawsuit challenging the general warrant. At trial, Chief Justice Pratt instructed the jury that if the government had the power to use general warrants, "it certainly may affect the person and property of every man in this kingdom, and is totally subversive of the liberty of the subject." n116 The jury found for Wilkes and the case became the stuff of legend. It was seen as an enormous victory for freedom of the press, and the British press ensured that news about the case was spread far and wide. n117 The number "45" was etched in chalk throughout London, and Benjamin Franklin noted after a visit that he observed a fifteen-mile stretch where "45" was marked on practically every door. n118 Hailed as a hero in Britain, Wilkes became a champion in the American colonies as well. n119 As Cuddihy observes: "Because American newspapers repeated whatever the British press reported on Wilkes and general **[*135]** warrants, those topics received the same saturation coverage in the colonies as in the mother country." n120

Two years after the Wilkes case, John Entick challenged a general warrant in a seditious libel investigation. Like Wilkes, Entick's home had been searched and his papers seized. In Entick v. Carrington, n121 Lord Camden, who was formerly Chief Justice Pratt and the author of the Wilkes opinion, issued a blistering critique of general warrants. Camden declared that with a general warrant, a person's "house is rifled; his most valuable secrets are taken out of his possession, before the paper for which he is charged is found to be criminal by any competent jurisdiction, and before he is convicted either of writing, publishing, or being concerned in the paper." n122 Word of the Entick case was also greeted with cheer in America, and Wilkes and Lord Camden were so venerated that towns were named in their honor. n123

William Stuntz suggests that Wilkes and Entick were so eminent because of their protection of First Amendment activities. Stuntz notes that restrictions on searches and seizures made it "harder to prosecute" political crimes such as seditious libel. n124 As Stuntz goes on to argue:

> Entick and Wilkes are classic First Amendment cases in a system with no First Amendment, no vehicle for direct substantive judicial review. Restricting paper searches had the effect of limiting government power in a class of cases that were, even at the time, deemed seriously troubling in substantive terms, as shown not only by Camden's remarks in Entick but also by the public's embrace of the two decisions. n125

Stuntz contends that the law of search and seizure is the "consequence of the strong tradition of using Fourth and Fifth Amendment law as a shield against government information gathering - a tradition that has **[*136]** more to do with protecting free speech than with regulating the police." n126

The origins of the Fifth Amendment privilege against self-incrimination are in considerable dispute. The Fifth Amendment privilege is based upon a privilege that arose at common law, n127 but there is significant disagreement as

to when and why it emerged. Leonard Levy traces the origins of the privilege to resistance to the practice of ex officio oaths in England in the Middle Ages. n128 Puritans and others who did not conform to the Church were forced to "answer upon their oath in causes against themselves - and also to answer interrogations touching their own contempts and crimes objected against them." n129 In mid-seventeenth-century England, John Lilburne's famous refusal to submit to the oath when accused of seditious libel led to an intense public distaste for the ex officio oath and its ultimate abolition in 1641. n130

Recent scholarship, however, has proposed an alternative theory of the creation of the privilege. John Langbein contends:

> The true origins of the common law privilege are to be found not in the high politics of the English revolutions, but in the rise of adversary criminal procedure at the end of the eighteenth century. The privilege against self-incrimination at common law was the work of defense counsel. n131

For a long time after their ratification, the Fourth and Fifth Amendments lay dormant, unexplored by the Supreme Court. But in **[*137]** the late nineteenth century, when the Supreme Court first interpreted the Fourth and Fifth Amendments, it turned to Wilkes and Entick.

Early Fourth and Fifth Amendment cases involved people's correspondence and papers. In 1878, in Ex Parte Jackson, n132 the Court held that the Fourth Amendment prohibited the government from opening mail: "The constitutional guaranty of the right of the people to be secure in their papers against unreasonable searches and seizures extends to their papers, thus closed against inspection, wherever they may be." n133 Ex Parte Jackson provided crucial protection for First Amendment activities, as the mail was an essential medium of communication at the time.

Ex Parte Jackson was a prelude to the 1886 case Boyd v. United States, n134 the most important Fourth and Fifth Amendment decision of the nineteenth century. In Boyd, law enforcement officials issued a subpoena in a civil forfeiture proceeding to compel Edward A. Boyd, a merchant, to produce invoices on cases of imported glass. As Stuntz notes, the Court viewed the subpoena as "the functional equivalent of a search or seizure" because it was "compelled rather than voluntary." n135

In its interpretation of the Fourth and Fifth Amendments, Boyd placed Wilkes and Entick at the center of constitutional criminal procedure. The Court noted that Entick was one of the "landmarks of English liberty" and "was welcomed and applauded by the lovers of liberty in the colonies as well as in the mother country." n136 Furthermore, the Court stated that Entick's "propositions were in the minds of those who framed the Fourth Amendment to the Constitution, and were considered as sufficiently explanatory of what was meant by unreasonable searches and seizures." n137 The Court then held that the subpoena violated the Fourth and Fifth Amendments:

> Breaking into a house and opening boxes and drawers are circumstances of aggravation; but any forcible and compulsory extortion of a man's own testimony or of his private papers to be used as evidence to convict him of crime or to forfeit his goods, is within the condemnation of [Lord Camden's] judgment. In this regard the Fourth and Fifth Amendments run almost into each other. n138

[*138] The Court declared that the Fourth and Fifth Amendments "throw great light on each other" and that "we have

been unable to perceive that the seizure of a man's private books and papers to be used in evidence against him is substantially different from compelling him to be a witness against himself." n139 Although Boyd did not mention the First Amendment, it functioned to protect a significant amount of First Amendment activity by guarding personal papers. n140

The days of Boyd have long come to an end. In 1967, with its decision in Warden v. Hayden, the Supreme Court began an assault on Boyd. n141 In several cases in the 1970s, the Court held that subpoenas to third parties for a person's papers do not implicate the Fifth Amendment. n142 Moreover, the Court concluded, subpoenas do not constitute a Fourth Amendment search. n143 The third-party doctrine and doctrine on public surveillance have also severely curtailed the Fourth Amendment's protection of personal writings, reading habits, associations, and other First Amendment activities. n144

2. Government Information Gathering from the Twentieth Century to the Present

Some might argue that the history of the First, Fourth, and Fifth Amendments is no longer relevant since seditious libel prosecutions no longer lurk as a major threat. But experiences in the twentieth century through the present demonstrate that government investigations continue to pose a substantial threat to First Amendment activity. Throughout the past century, the government has gathered information about activities protected by the First Amendment in troubling ways. n145 Between 1940 and 1973, the FBI and CIA secretly **[*139]** read the mail of thousands of people. n146 The FBI has engaged in extensive surveillance of student political and speech activities on college campuses. n147 During the 1980s, through the "Library Awareness Program," the FBI gathered information from people's library records. n148

During the McCarthy era, from 1946-1956, the FBI gathered extensive information about Communist Party members for use in Congress's inquest into the Party. n149 As Ellen Schrecker has observed, "the FBI was the bureaucratic heart of the McCarthy era. It designed and ran much of the machinery of political repression, shaping the loyalty programs, criminal prosecutions, and undercover operations that pushed the communist issue to the center of American politics during the early years of the Cold War." n150 In the 1950s, the FBI maintained a "Security Index" of about 26,000 individuals to round up in case of a national security emergency. n151 The FBI also used a network of informers to infiltrate the Communist Party. n152

From 1956 to 1971, the FBI engaged in a massive attempt to gather information about scores of political groups as part of its Counterintelligence Program known as COINTELPRO. n153 Among the targets were the Communist Party, the Ku Klux Klan, antiwar groups, civil rights groups, women's rights groups, and gay rights groups. n154 The FBI used the data it collected to hinder the activities **[*140]** of these groups. n155 It engaged in zealous surveillance of the civil rights movement, especially focusing on Martin Luther King, Jr. n156 Over a span of many years, the FBI wiretapped King extensively and attempted to use the recordings to threaten and intimidate him. n157

In 1975, a congressional committee led by Senator Frank Church (and thus known as the Church Committee) began a sweeping inquiry into intelligence abuses. In its 1976 report (the Church Committee Report), the Church Committee stated:

The Government, operating primarily through secret informants, but also using other intrusive techniques such as wiretaps, microphone "bugs," surreptitious mail opening, and break-ins, has swept in vast amounts of information about the personal lives, views, and associations of American citizens... . Groups and individuals have been harassed and disrupted because of their political views and their lifestyles. Investigations have been based upon vague standards whose breadth made excessive collection inevitable. n158

In response to the Church Committee Report, Attorney General Edward Levi established a set of guidelines for FBI investigations in 1976. n159 The guidelines specifically addressed First Amendment activities: "First, investigations based solely on unpopular speech, where there is no threat of violence, were prohibited. Second, techniques designed to disrupt organizations engaged in protected First Amendment activity, or to discredit individuals would not be used in any circumstance." n160

However, under the pressure of a new wave of concerns about national security, the protections of the guidelines have been slowly dismantled. In 1983, Attorney General William French Smith revised the guidelines to create a lower threshold to open an investigation. n161 After the September 11th attacks, Attorney General John Ashcroft made numerous changes to the guidelines. Among other things, the new guidelines allow the FBI to gather "publicly available information, **[*141]** whether obtained directly or through services or resources (whether nonprofit or commercial) that compile or analyze such information; and information voluntarily provided by private entities." n162 The FBI can also "carry out general topical research, including conducting online searches and accessing online sites and forums." n163

Today, government information gathering - especially in the name of national security - remains a significant threat to First Amendment activities. In response to the threat of terrorism, the NSA has engaged in warrantless wiretapping of telephone calls; government agencies have increased their demands for personal information maintained in business records; the government has gathered extensive information about financial transactions; and numerous data mining programs have involved the collection of massive amounts of personal information. n164 These data gathering programs have occurred under a veil of secrecy, but it is nonetheless clear that monitoring telephone calls, analyzing financial transactions, and mining other personal data likely will yield information relating to conversations, religious and political activity, and group associations.

While legitimate investigation of terrorist plots may require collecting and examining data about communication and association, the implications for First Amendment activities advise caution. In the famous Keith case, n165 Justice Powell wrote that "national security cases ... often reflect a convergence of First and Fourth Amendment values not present in cases of 'ordinary' crime. Though the investigative duty of the executive may be stronger in such cases, so also is there greater jeopardy to constitutionally protected speech." n166 With the lack of transparency surrounding information gathering in the name of national security, it is difficult to find out precisely what makes a particular person suspicious and how people's First Amendment **[*142]** activities might turn them into targets of investigation. People might be targeted on the basis of their political views, religious beliefs, and associations. Even if First Amendment activities play no role in these determinations, people may nonetheless be reticent to say certain things, worship in certain places, associate with certain groups, or even read certain materials out of fear that they might end up on a list of suspicious persons. n167 As David Cole observes, during the McCarthy era, "most 'radicals' were punished not for their speech but for their membership, affiliation, or sympathetic association with the Communist Party." n168

The history of government information gathering in the twentieth century thus suggests that even though concerns raised by seditious libel may have faded, government investigation practices can still pose a significant threat to First Amendment activities. Relying on government investigators to police themselves in those areas that are unprotected by current criminal procedure law is highly risky in light of the historical record. Developing First Amendment protections against government information gathering would add a vital and missing dimension to the current landscape of criminal procedure.

B. Foundations in Doctrine

Several lines of First Amendment cases provide a foundation on which to develop First Amendment criminal procedure. The Supreme Court has noted that "governmental action may be subject to constitutional challenge even though it has only an indirect effect on the exercise of First Amendment rights," n169 and government information gathering will often indirectly affect the exercise of First Amendment rights by discouraging expressive and associational activity. Indirect effects on First Amendment activities are addressed through the "chilling effect" doctrine. The chilling effect doctrine recognizes that the First Amendment can be implicated indirectly and not just

through direct legal prohibitions on speech. n170 The key to chilling effect is deterrence: "A chilling effect occurs when individuals seeking to **[*143]** engage in activity protected by the First Amendment are deterred from so doing by governmental regulation not specifically directed at that protected activity." n171

Courts have concluded that government information gathering indirectly inhibits or "chills" First Amendment liberties in a wide range of contexts, including surveillance of political activities, identification of anonymous speakers, prevention of the anonymous consumption of ideas, discovery of associational ties to political groups, and enforcement of subpoenas to the press or to third parties for information about reading habits and speech. While the cases addressing these issues are mostly civil, their principles are just as relevant and applicable to criminal cases and to government information gathering for national security and other purposes.

1. Surveillance of Political Activities

Courts sometimes have found that government surveillance of political activities can implicate the First Amendment. The Supreme Court confronted this issue in a 1972 case, Laird v. Tatum, n172 in which a group of individuals brought a First Amendment challenge to the Department of the Army's surveillance of civil rights activities in the aftermath of Martin Luther King, Jr.'s assassination. The Army had harvested information on political activities from news reports and from intelligence agents who attended public meetings. n173 While acknowledging that "constitutional violations may arise from the deterrent, or 'chilling,' effect of governmental regulations that fall short of a direct prohibition against the exercise of First Amendment rights," n174 the Court nonetheless concluded that the plaintiffs failed to establish a cognizable First Amendment injury because "allegations of a subjective 'chill' are not an adequate substitute for a claim of specific present objective harm or a threat of specific future harm." n175

Laird was not especially clear about when government surveillance (and information gathering practices more generally) will cause a cognizable First Amendment injury. Indeed, one view of Laird interprets it as a very narrow, fact-specific holding based on the plaintiffs' highly tenuous First Amendment injury. The Court concluded that the plaintiffs merely articulated "speculative apprehensiveness that the Army may at some future date misuse the information in **[*144]** some way that would cause direct harm to respondents." n176 In other words, Laird might be read to state only that naked allegations of "speculative apprehensiveness" are insufficient to establish a cognizable chilling effect.

Lower courts have interpreted Laird to mean that the mere presence of the police or recording of information at public meetings do not constitute cognizable First Amendment injuries. n177 However, when plaintiffs have produced evidence of deterrence (as opposed to mere allegations of discomfort or dislike), courts have found cognizable First Amendment injuries. n178 In addition, several courts have distinguished Laird when the government surveillance went beyond public meetings to closed and private meetings. n179 Other courts have distinguished Laird when plaintiffs alleged that the police not only collected information but also used it in harmful ways. n180 Therefore, the rule in Laird can be limited to situations involving mere allegations of government information gathering in public meetings without **[*145]** any evidence of deterrence or any indication of palpable harmful future uses of the information.

2. Identifying Anonymous Speakers

The Supreme Court has held that restrictions on the ability to speak anonymously violate the First Amendment. In Talley v. California, n181 the Court held that a law prohibiting the distribution of anonymous handbills violated the First Amendment. n182 The Court reasoned that anonymity is essential to protecting robust and uninhibited speech, and it noted that the "old seditious libel cases in England show the lengths to which government had to go to find out who was responsible for books that were obnoxious to the rulers." n183 As the Court declared in 1995 in reaffirming its protection of anonymity in McIntyre v. Ohio Elections Commission, n184 an author's "decision in favor of anonymity may be motivated by fear of economic or official retaliation, by concern about social ostracism, or merely by a desire to preserve as much of one's privacy as possible." n185

The right to speak anonymously is implicated when the government seeks to obtain ISP records that can identify anonymous speakers on the Internet. n186 In several lower court decisions, courts have used heightened standards for civil subpoenas requesting the identities of anonymous speakers. For example, in Doe v. 2TheMart. com Inc., n187 the court noted:

The free exchange of ideas on the Internet is driven in large part by the ability of Internet users to communicate anonymously. If Internet users could be stripped of that anonymity by a civil subpoena enforced under the liberal rules of civil discovery, this would have a significant chilling effect on Internet communication and thus on basic First Amendment rights. n188

[*146] Numerous other cases have concluded that the First Amendment requires special, tougher standards before a subpoena can be enforced to reveal an anonymous speaker's identity. n189

3. Curtailing the Right to Receive Ideas

A corollary to the right to free speech is the right to receive ideas. In Stanley v. Georgia, n190 the Court declared: "It is now well established that the Constitution protects the right to receive information and ideas... . This right to receive information and ideas, regardless of their social worth, is fundamental to our free society." n191 Government information gathering can target information about the ideas a person is consuming. Subpoenas for library or bookstore records can reveal what books a person reads, and subpoenas to ISPs also implicate the right to receive ideas. As Julie Cohen contends, "The freedom to read anonymously is just as much a part of our tradition, and the choice of reading materials just as expressive of identity, as the decision to use or withhold one's name." n192

The Supreme Court has also held that disallowing an individual from anonymously consuming ideas places an unconstitutional burden on First Amendment rights. For example, in Lamont v. Postmaster General, n193 the Court struck down on First Amendment grounds a statute that required that foreign mail deemed "communist political propaganda" be kept at the post office, with the addressee having to make a special request to receive it. The Court reasoned that having to "request in writing that [one's mail] be delivered" was "almost certain to have a deterrent effect." n194 Under such a system, people are "likely to feel some inhibition in sending for literature which federal officials have condemned as 'communist political propaganda.'" n195

[*147] Several lower courts have required a "compelling interest" for any subpoena pertaining to First Amendment activities, such as one's reading habits or speech. n196 For example, in In re Grand Jury Subpoena to Kramerbooks & Afterwords Inc., n197 Independent Counsel Kenneth Starr, in his investigation of President Bill Clinton, subpoenaed records relating to Monica Lewinsky's book purchases at Kramerbooks and Barnes & Noble. Kramerbooks challenged the subpoena on First Amendment grounds. The court concluded that First Amendment activities, namely the "right to receive information and ideas," were implicated by the subpoenas. n198 Accordingly, in order to determine whether a "compelling need" was present, the court ordered that the Office of Independent Counsel submit a "filing describing its need for the materials sought by the subpoenas to Kramerbooks and Barnes & Noble and the connection between the information sought and the grand jury investigation ... ." n199

4. Revealing Associational Ties to Political Groups

Government information gathering about people's associations can also trigger First Amendment scrutiny. The Supreme Court has concluded that the First Amendment protects "expressive" association, which is association for the purpose of engaging in expressive activities. n200 In NAACP v. Alabama ex rel. Patterson, n201 the Court held that the NAACP could not be compelled to publicly disclose the names and addresses of its members. The Court declared that

"freedom to engage in association for the advancement of beliefs and ideas is an inseparable aspect of the 'liberty' assured by the Due Process **[*148]** Clause of the Fourteenth Amendment, which embraces freedom of speech." n202 Noting that there is a "vital relationship between freedom to associate and privacy in one's associations," n203 the Court went on to conclude that exposing members' identities would subject them "to economic reprisal, loss of employment, threat of physical coercion, and other manifestations of public hostility." n204

The Court reached similar conclusions in Bates v. City of Little Rock n205 and Gibson v. Florida Legislative Investigation Committee, n206 cases also involving the compulsory public disclosure of NAACP membership lists. In Buckley v. Valeo, n207 the Court applied "exacting scrutiny" to disclosure requirements for certain campaign contributions and expenditures under the Federal Election Campaign Act of 1971. n208 Although ultimately upholding the law as to contribution limits, the Court noted that "it is undoubtedly true that public disclosure of contributions to candidates and political parties will deter some individuals who otherwise might contribute." n209

The Court has also held that First Amendment rights are implicated when information about an individual's associations is compelled by the government, even if no public disclosure is threatened. In Sweezy v. New Hampshire, n210 the Court held that a state attorney general could not compel a witness before a state legislature to divulge his associations with particular Communist organizations: "Merely to summon a witness and compel him, against his will, to disclose the nature of his past expressions and associations is a measure of governmental interference in these matters." n211 In Shelton v. Tucker, n212 moreover, the Court invalidated a statute that required instructors to file an annual affidavit "listing without limitation every organization to which [they had] belonged or regularly contributed within the preceding five years" as a condition of employment in a **[*149]** state school or college. n213 The Court concluded that "the statute's comprehensive interference with associational freedom goes far beyond what might be justified in the exercise of the State's legitimate inquiry into the fitness and competency of its teachers." n214 In particular, the Court was troubled by the breadth of the inquiry, which extended to "every conceivable kind of associational tie - social, professional, political, avocational, or religious." n215 The Court reached a similar conclusion in Baird v. State Bar of Arizona, n216 finding that questioning a bar applicant about membership in any organization "that advocated overthrow of the United States Government by force or violence" infringed on freedom of association. n217

These Supreme Court cases all involved direct interrogation, but their logic could apply to searches and subpoenas for papers and documents. Lower federal courts applying Baird, Sweezy, and Shelton have found that subpoenas for associational information implicate the First Amendment. n218 The case law thus suggests that the government creates indirect burdens on free association when it seeks information about a person's expressive associations. The mere collection of information on association by the government can be sufficient to establish a First Amendment injury.

[*150]

5. Subpoenas to the Press

First Amendment doctrine also protects against government information gathering directed toward the press, though the limits of this protection are still unclear. In Branzburg v. Hayes, n219 journalists raised First Amendment challenges to subpoenas to testify before grand juries about the identities of several sources for their stories. While the Court concluded journalists did not enjoy a special First Amendment privilege to refuse to testify before the grand jury about their sources, n220 it also noted:

News gathering is not without its First Amendment protections, and grand jury investigations if instituted or conducted other than in good faith, would pose wholly different issues for resolution under the First Amendment... . Grand juries are subject to judicial control and subpoenas to motions to quash. We do not expect courts will forget that grand juries must operate within the limits of the First Amendment as well as the Fifth. n221

The majority opinion in Branzburg thus acknowledged the First Amendment values implicated by forcing reporters to testify before grand juries but refused to create an explicit reporter's privilege.

Swing voter Justice Powell's concurrence offered up an interpretation of the majority holding that suggested somewhat stronger First Amendment protections. Powell noted that the "Court does not hold that newsmen, subpoenaed to testify before a grand jury, are without constitutional rights with respect to the gathering of news or in safeguarding their sources." n222 Rather, "the courts will be available to newsmen under circumstances where legitimate First Amendment interests require protection." n223 He went on to argue that privilege claims should be assessed "by the striking of a proper balance between freedom of the press and the obligation of all citizens to give relevant testimony with respect to criminal conduct." n224

Despite the conflict between the majority opinion and the concurrence, n225 the "overwhelming numbers of state and federal courts **[*151]** have interpreted Branzburg, and the subsequent Supreme Court decisions that have had occasion to revisit it, as recognizing in the First Amendment a qualified journalists' privilege." n226 Accordingly, the majority of courts balance the interest in protecting freedom of the press against the interest in compelling testimony about confidential sources to determine whether compelling a journalist to testify passes constitutional muster. n227

* * * Taken together, these many lines of First Amendment cases establish a foundation for First Amendment protection against certain instances of government information gathering. The cases recognize that government information gathering through surveillance, subpoenas, questioning, and other techniques can chill freedom of speech, consumption of ideas, association, and other rights. First Amendment criminal procedure thus has substantial roots in existing First Amendment doctrine.

III

Contours and Applications

As I have shown, current criminal procedure leaves much First Amendment activity unprotected. n228 I have argued that based on its history, values, and doctrine, the First Amendment should serve as an independent source of procedure to protect expressive and associational activity from government information gathering. Any theory of First Amendment criminal procedure will have to determine when the First Amendment applies to a government investigation and, if it applies, what types of procedures are required. In this part, I set forth an approach to First Amendment criminal procedure, and I explore how this approach would work by applying it to several examples.

A. When Should the First Amendment Apply?

When should government information gathering trigger First Amendment protection? The answer depends upon the resolution of two questions:

[*152] (1) Does the government information gathering affect activities that fall within the boundaries of the First Amendment?

(2) Does it have a chilling effect upon such activities?

1. First Amendment Boundaries

In determining whether the First Amendment regulates an instance of government information gathering, the first question is whether it implicates an activity that falls within the boundaries of the First Amendment. To make this determination, we cannot simply ask whether a particular law enforcement investigation implicates expressive or

associational activity, as nearly all law enforcement investigations do. Instead, we must ask whether First Amendment values are implicated.

The First Amendment currently covers a veritable kingdom of territory, so it is often not implausible to find the First Amendment implicated by a wide array of government conduct. Almost every search or seizure could be understood to have some dimension that might involve a First Amendment activity because all human interaction involves communication and association. n229 In the end, the First Amendment could swallow up all of criminal procedure.

Moreover, some commentators have argued that First Amendment coverage is not only broad, but cannot be contained by any limiting principle. As Frederick Schauer aptly observes, "if there exists a single theory that can explain the First Amendment's coverage, it has not yet been found." n230 According to Schauer:

> Little case law and not much more commentary explain why the content-based restrictions of speech in the Securities Act of 1933, the Sherman Antitrust Act, the National Labor Relations Act, the Uniform Commercial Code, the law of fraud, conspiracy law, the law of evidence, and countless other areas of statutory and common law do not, at the least, present serious First Amendment issues. n231

> Schauer notes that First Amendment "coverage may often be a function simply of the persistent visibility of First Amendment rhetoric, and noncoverage may conversely be a function of the failure of such rhetoric to take hold." n232

[*153] To overcome this problem, First Amendment criminal procedure should adopt the approach suggested by Robert Post and look to whether a particular government activity implicates First Amendment values. n233 Post argues that not all communications are expressive in ways that promote First Amendment values. For example, he observes that navigation charts "are clearly media in which speakers successfully communicate particularized messages," but "when inaccurate charts cause accidents, courts do not conceptualize suits against the charts' authors as raising First Amendment questions." n234 According to Post, to determine the scope of the First Amendment we must examine "the social contexts that envelop and give constitutional significance to acts of communication." n235

Thus, in determining whether an instance of government information gathering implicates the First Amendment, we cannot merely look to whether a particular instance of government information gathering has any possible expressive or associational dimensions, but also to whether the expressive or associational dimension implicates the values that the First Amendment protects. The First Amendment protects communication, association, and other activities when they implicate belief, discourse, or relationships of a political, cultural, or religious nature. The Supreme Court itself has recognized that some expressive and associational activity is less central to, or not protected at all by, the First Amendment. Obscenity, n236 fighting words, n237 and child pornography n238 are considered low-value speech and receive diminished First Amendment protection. The Court has also not considered conspiracy, quid pro quo sexual harassment, insider trading, and other forms of communicative activity to be protected speech. n239

[*154] Looking to First Amendment values prevents the First Amendment from unduly limiting government information gathering in other contexts. For example, government collection of business records would generally not trigger First Amendment restrictions. In the days when Boyd barred most paper searches, the Court in Hale v. Henkel n240 concluded that subpoenas for corporate documents were not restricted by the Fourth Amendment. n241 The First Amendment also does not apply to a large dimension of business regulation, even when companies must disclose records to regulators. In other words, First Amendment law has adopted, at least in part, the Fourth Amendment distinction between personal and business papers.

In sum, First Amendment criminal procedure protections should not apply whenever any expressive or associational activity is involved but only when such activity implicates values protected by the First Amendment.

2. Chilling Effect

Even where government information gathering implicates First Amendment values, First Amendment procedural protections should only apply if there is a discernible "chilling effect." As with determining whether an activity falls within the scope of the First Amendment, the challenge is defining the boundaries of "chilling effect." Schauer has observed that all government action can have some chilling effect; "what we must look for is some way of determining under what circumstances the inevitable chilling effect becomes great enough to require judicial invalidation of legislative enactments" or executive information gathering. n242 We need an approach for distinguishing between cognizable and noncognizable chilling effects. The **[*155]** chilling effect cases unfortunately do not provide a clear approach to the problem. n243

Determining the existence of a chilling effect is complicated by the difficulty of defining and identifying deterrence. It is hard to measure the deterrence caused by a chilling effect because it is impossible to determine with certainty what people would have said or done in the absence of the government activity. Often, the primary evidence will be a person's own assertions that she was chilled, but merely accepting such assertions at face value would allow anyone claiming a chilling effect to establish one. At the same time, demanding empirical evidence of deterrence is impractical because it will often be impossible to produce.

In order to deal with this problem, courts have allowed some speculation about deterrence but have required more than mere apprehensiveness. While the case law is somewhat muddled, the Supreme Court is prepared to recognize a cognizable chilling effect from the imposition of civil damages, as in defamation cases, n244 or from public disclosure of information gathered by the government, as sometimes occurs in association cases. n245 Although in some cases exposure of information to the government alone can trigger a chilling effect - for example, in cases involving anonymous expression or associations n246 - in many other instances, as with surveillance of public meetings, such exposure is not, by itself, sufficient. n247

In freedom of association cases, the Court may be especially willing to find a chilling effect. In NAACP v. Alabama ex rel. Patterson, n248 the NAACP did not need to proffer statistics about declining membership. Instead, it could point to palpable consequences that were likely (though not certain) to follow from the government's actions. n249 In other freedom of association cases, the Court has concluded that mere government collection of information about associations was sufficient to create a cognizable First Amendment injury. n250

[*156] At a minimum, use of previously gathered information in a criminal prosecution would be sufficient to show deterrence. In many cases involving government information gathering about First Amendment activities, the government is collecting data to generate evidence for use in criminal cases. In Dombrowski v. Pfister, n251 the Court found First Amendment standing based on the threat of criminal prosecution because "the chilling effect on the exercise of First Amendment rights may derive from the fact of the prosecution, unaffected by the prospects of its success or failure." n252

Dombrowski involved a statute that directly targeted free expression and political activity, n253 but similar chilling effects can also occur when the government is investigating non-speech-related crimes. Many government investigations implicating First Amendment interests will be for the prosecution of crimes such as conspiracy, murder, robbery, or computer hacking, and not for crimes based on the illegality of speech or association. Even where the criminalized activity is not itself expressive or associational, there may be a chilling effect sufficient to trigger First Amendment procedural protections. People might be chilled in writing or saying certain things, owning certain books, visiting particular websites, or communicating with particular individuals, groups, and organizations if the government can obtain and use information about these activities in a criminal prosecution. A person might not want to purchase a book about making bombs or flying a plane if it will be used against him or her in a trial for conspiracy to engage in

terrorist acts. A person might not go to various religious or political websites if she knew that the government might use this as evidence in such a case. Even if there were no criminal case brought, the fear that engaging in First Amendment activities might trigger an arrest or a potential criminal probe might be sufficiently daunting to chill such activities. Whether criminal investigation alone is sufficient to create a chilling effect will depend upon the specific facts of each case, including whether the person being investigated can demonstrate deterrence of First Amendment activities.

In contrast, certain government information gathering activities for criminal investigations may not have a chilling effect. Under existing First Amendment doctrine, when the government merely gathers information that is widely exposed to the public, there is no **[*157]** cognizable chilling effect. n254 For example, suppose a person publishes a political manifesto, and an FBI agent purchases it in a bookstore. n255 Although this is government information gathering for the purpose of finding out about the person's speech, the First Amendment should not apply because the book was written for public consumption. In contrast, a violation of the First Amendment might occur if law enforcement authorities read private writings that were shared with a small group of people, but not with the public at large. Similarly, limited surveillance of activities visible to the public would most likely not trigger First Amendment protection, but a more systematic campaign of public surveillance might present a different situation.

Criminal investigations and prosecutions are not the only potential source of chilling effects. In many instances, the government engages in broad information gathering that is not directly tied to a concrete penalty or consequence, but which still may chill speech. For example, people might fear that if the government learns about their speech or associations, they will wind up on a terrorist watch list. However, they might never know if they are in fact on a watch list, and the consequences of being placed on such a list might be unclear. Being placed on a watch list might result in extra airline screening, or it might have no impact on the individual at all. Or the information could go into a government database for some unknown future use when the time is ripe.

These uses are speculative, and they present a difficult case for chilling effect analysis. Courts might conclude that people should wait to see how the information is used; if the government uses their information against them, defendants would then be able to allege a cognizable chilling effect. However, this ignores the central premise of the chilling effect doctrine - that many will not be willing to accept the risk and will instead simply change their behavior. Therefore, even if the information is never used at trial, uncertainty about the government's intentions may still deter First Amendment activities. The government might argue that it must keep secret the uses of the information it gathers, but this only exacerbates the problem - lack of transparency makes it especially difficult for individuals to allege a sufficiently concrete chilling effect. By collecting data and obscuring its potential uses, the government can effectively limit people's ability to assert their First Amendment rights by making it impossible for them to establish a sufficient chill.

[*158] The First Amendment concept of overbreadth might provide a solution to the problems presented by situations involving such large-scale information gathering programs. According to the Supreme Court, "a governmental purpose to control or prevent activities constitutionally subject to state regulation may not be achieved by means which sweep unnecessarily broadly and thereby invade the area of protected freedoms." n256 Overbreadth doctrine relaxes the normal standing rules to allow people to bring suit without having to show that the law is unconstitutional as applied to them. n257 To challenge a statute as overbroad, an individual need only show that some application of the law is unconstitutional and might chill the speech of parties not before the court. For a statute "to be facially challenged on overbreadth grounds" there "must be a realistic danger that the statute itself will significantly compromise recognized First Amendment protections of parties not before the Court." n258

The concept of overbreadth in connection with government information gathering has a close analogue in the Fourth Amendment's concept of particularity, which mandates procedures to prevent overbroad searches. The Fourth Amendment requires that a warrant must describe with "particularity ... the place to be searched, and the persons or things to be seized." n259 The Framers included the particularity requirement because they wanted to restrict general warrants and writs of assistance. n260 Writs of assistance were pernicious because they allowed "sweeping searches and seizures without any evidentiary basis." n261 General warrants "resulted in 'ransacking' and seizure of the personal

papers of political dissidents, authors, and printers of seditious libel." n262 Overbreadth is therefore not a concept foreign to criminal procedure.

[*159] We can adapt overbreadth doctrine to address the problem of proving a chilling effect when the government engages in large-scale information gathering initiatives. In this context, litigants could challenge an information gathering program as overbroad, regardless of whether they could prove that they personally suffered a concrete chilling effect. Instead, courts would determine whether the government program sweeps so broadly that it captures a substantial amount of First Amendment activity. A program that sweeps in a great deal of First Amendment activity will be deemed unconstitutionally overbroad if not narrowly tailored to a substantial government interest. Allowing such challenges will have the secondary benefit of bringing greater transparency to information gathering programs, as the government will be forced to justify its activities and the breadth of their scope.

In sum, to determine whether First Amendment procedural protections will apply, courts should first look to see whether the activity at issue is within the scope of the First Amendment. Next, courts must determine whether the government information gathering has a cognizable chilling effect on First Amendment activity. Criminal prosecutions will almost always have some chilling effect. In situations involving large-scale programs, litigants should be able to bring overbreadth challenges without having to prove individual chilling effect.

B. What Level of Protection Should the First Amendment Require?

Even if an instance of government information gathering triggers First Amendment protection, collection of the data will not necessarily be prohibited. Rather, the First Amendment will require the government to demonstrate (1) a significant interest in gathering the information and (2) that the manner of collection is narrowly tailored to achieving that interest. As I will discuss in this Section, the use of a warrant supported by probable cause will, in most cases, suffice to satisfy the narrow tailoring requirement. In other words, in cases where the First Amendment applies, it often will require procedures similar to those required by the Fourth Amendment.

1. First Amendment Information Gathering Procedures

If the First Amendment is implicated by government information gathering, how should it regulate the government's activities? Under one possible approach, the First Amendment might serve as an absolute prohibition, preventing the government from gathering data involving First Amendment activities. For example, Michael Mello and Paul Perkins have argued that the contents of a diary "are entitled **[*160]** to absolute protection from governmental intrusion - regardless of how much probable cause the government possesses, and regardless of how many procedurally valid search warrants the government obtains." n263

However, such an approach is impractical. First Amendment protection involves balancing, n264 and it need not absolutely bar the government from engaging in information gathering. In general, First Amendment balancing begins by assessing the strength of the government interest. If the government interest is compelling or substantial, the court then analyzes whether the government action is sufficiently narrowly tailored to the achievement of the government interest. n265

Under my approach, the same standard would apply to government investigations. When the First Amendment applies, the government information gathering would only be upheld if it serves a substantial government interest and employs narrowly tailored means to achieve that interest. The First Amendment would rarely completely ban a particular instance of government information gathering. Instead, the court would balance the need for unencumbered government information gathering against the impact on First Amendment rights. If the government interest is substantial, the First Amendment would mandate procedures that must be followed in order for the information gathering to take place, such as obtaining a warrant.

On the first question, the government must be able to establish a substantial interest in the information or it will be

restricted by the First Amendment from engaging in its investigation. For example, investigating serious crimes and preventing terrorism would qualify as substantial. This part of the balancing approach would root out government information gathering initiatives that lack a compelling purpose. It would also force the government to be more transparent about the reasons for its information gathering activities.

A court would then analyze whether the means used to gather the information were narrowly tailored to achieve the government's interest. Courts would look to whether the information gathering effectively furthers the government's interest, and whether the procedural **[*161]** safeguards and judicial oversight available are sufficient to prevent abuse without rendering the investigation ineffective. n266

In many cases, if applicable, the First Amendment would require that information be gathered pursuant to a warrant and probable cause. Warrants and probable cause have several attributes that will help safeguard First Amendment activities. First, warrants prevent government information gathering from becoming excessively broad by requiring that government officials specify with "particularity ... the place to be searched, and the persons or things to be seized." n267 Second, warrants require judicial oversight of the executive branch's law enforcement activities, thus serving as a check against interference with First Amendment activities. Warrants require the government to justify its search in advance, thereby preventing it from "dreaming up post hoc rationalizations." n268 By the same token, advance justification for information gathering prevents the government from searching people because of disfavored speech or associations in order to uncover evidence that could be used to prosecute them for unrelated offenses. Third, by requiring that government officials "document their requests for authorization," warrants force officials to exercise more circumspection in deciding when to gather information. n269 Fourth, the probable cause requirement prevents information gathering based on the mere hunch or whim of government officials; it prevents the government from searching people merely because their associations, expression, or beliefs are unpopular. n270 Under my First Amendment approach, law enforcement officials would apply for a search warrant in much the same way they do under the Fourth Amendment. In other words, we would see the birth of what might be called the "First Amendment warrant."

Some might argue that a warrant requirement would not adequately protect First Amendment interests. In fact, a case decided in 2002 by the Colorado Supreme Court directly examined this issue. In **[*162]** Tattered Cover, Inc. v. City of Thornton, n271 police officers searching a methamphetamine lab seized two "how to" books about operating drug laboratories. The officers also found an envelope and invoice from the Tattered Cover bookstore and subsequently obtained a search warrant to examine the bookstore's records for the books the suspect purchased. The bookstore challenged the warrant under the First Amendment and the Colorado Constitution. The Colorado Supreme Court agreed that the warrant was not enforceable and should not have been issued. n272 The court reasoned that gathering information about reading habits infringes "the First Amendment rights of customers and bookstores because compelled disclosure of book-buying records threatens to destroy the anonymity upon which many customers depend." n273 The court held that the Colorado Constitution requires that "law enforcement officials must make a heightened showing of their need for the innocent bookstore's customer purchase records." n274 The court then rejected the warrant because the gathered evidence was not sufficiently important to the prosecution's case to justify the chilling effect that execution of the warrant would cause. n275

While in many cases the warrant and probable cause requirements would adequately protect First Amendment activities, there may be some instances when the Tattered Cover case's approach would be preferable. In some circumstances, warrants will not provide the optimal protection to First Amendment activities. Warrants enable the police to look around in their search for particular papers, increasing the risk that they will discover other documents. In addition, unlike with subpoenas, people cannot challenge warrants beforehand. But Zurcher forecloses stronger protections than warrants under the United States Constitution. n276 Nonetheless, although warrants are not perfect, they still provide significant protections for First Amendment activities.

Eugene Volokh has criticized attempts to raise the threshold requirements for law enforcement officials to obtain information about First Amendment activities. Pointing out the great difficulties in establishing an appropriate standard, he argues that a higher bar **[*163]** will "dramatically interfere with the investigation of many crimes and torts,

especially those that have an ideological motive." n277 Furthermore, to the extent the law requires only a marginally higher threshold, it will not prevent chilling effects. n278

Although Volokh is certainly correct to note that setting the right standard is difficult, the warrant requirement is a workable standard that has a proven track record. Warrants are not so difficult to obtain that they prevent effective government investigations, yet they still require law enforcement officials to justify information gathering endeavors. The warrant requirement will subject many currently unregulated government information gathering activities to judicial oversight, creating accountability and preventing overreaching executive power.

2. Enforcement of First Amendment Rights

If the government gathers information in violation of the First Amendment, what remedies should the First Amendment provide? To start, if the government seeks to introduce improperly gathered information in a criminal trial, the First Amendment should require that the evidence be excluded. This is, of course, the typical Fourth Amendment enforcement mechanism for failure to obtain a valid warrant. Information obtained in violation of the First Amendment would be suppressed at trial, though most of the Fourth Amendment warrant exceptions, such as exigency and consent, would apply to First Amendment warrants as well.

Some might object that the First Amendment should not borrow from the Fourth Amendment's toolkit. While warrants and probable cause are mentioned in the Fourth Amendment, no specific procedural requirement is discussed in the First. Nor is there currently an exclusionary rule for First Amendment violations. However, the lack of a textual basis under the First Amendment should not preclude importing warrants, probable cause, the exclusionary rule, and other concepts from the Fourth Amendment. The Fourth Amendment's exclusionary rule was shaped in Weeks v. United States and is not based on the text of the Amendment. n279 It is not at all unprecedented for the Court to pollinate one amendment with concepts from **[*164]** another. For example, in Mapp v. Ohio, the Court extended the Fourth Amendment exclusionary rule to the states, n280 and justified its holding by importing concepts from the Fifth Amendment and noting the "intimate relation" between the Amendments. n281 The Court observed that "the philosophy of each Amendment and of each freedom is complementary to, although not dependent upon, that of the other in its sphere of influence - the very least that together they assure in either sphere is that no man is to be convicted on unconstitutional evidence." n282 A close relationship also exists between the First and Fourth Amendments. For example, Zurcher and the other scrupulous exactitude cases explicitly look to Fourth Amendment procedures to protect First Amendment rights. n283 The logic of these cases could easily be expanded to include not only warrants and probable cause, but also the exclusionary rule and other Fourth Amendment protections.

Therefore, in the event that the government seeks to use information obtained in violation of the First Amendment as evidence in a criminal trial, the exclusionary rule could serve as a viable way to enforce First Amendment protections. When the government wants to use the fruits of its information gathering in criminal trials, the sanction of exclusion will provide the necessary incentive to seek prior judicial approval through a warrant.

These protections, however, will not cover the many instances where there is no criminal case brought against the person whose First Amendment rights are infringed. Suppose, for example, the government subpoenas John Doe's diary because it contains evidence that will assist in the prosecution of another person. Doe's First Amendment rights might be implicated, but he is not the subject of the criminal probe. In this instance, Doe should be allowed to initiate a civil action to quash the subpoena or block the government from gathering the information. The court would then require the government to make a showing of probable cause in order to obtain the information. If Doe is not able to challenge the information gathering prior to its occurrence, then he could seek damages in a subsequent lawsuit.

In other instances, individuals' First Amendment rights may be implicated by broad information gathering programs that do not result **[*165]** in the use of data in criminal trials. In these cases, overbreadth doctrine would allow individuals to sue by demonstrating that the information gathering has a chilling effect on the exercise of First Amendment rights. n284 The First Amendment could also allow for flexibility in crafting other remedies. In cases

involving dragnet searches with no foreseeable threat of criminal prosecution, the exclusionary rule obviously will be ineffective as a remedy. Under these circumstances, a suit for injunctive relief might be more appropriate. The injunctive relief need not bring a government investigation completely to a halt. Courts might narrow an overly broad information gathering program rather than simply enjoin it, or impose certain minimization procedures. n285

Making the First Amendment an independent source of criminal procedure will thereby bring judicial scrutiny to government information gathering that has an impact on First Amendment activities and will force consideration of First Amendment values in the balance between security and liberty, in the context of criminal trials and beyond.

C. Applications

In the previous Sections, I have set forth an approach to applying the First Amendment in the criminal procedure context. First, courts should determine whether the First Amendment applies, a determination that involves analyzing whether the government information gathering implicates activity within the First Amendment's scope of protection and whether it has a sufficient chilling effect on the First Amendment activity. Second, if the First Amendment applies, courts must determine whether the government had a significant interest in gathering the information, and, if so, whether the process was narrowly tailored to the government interest. Under most circumstances, this will require the government to obtain a warrant supported by probable cause in order to collect the information. Improperly gathered data can be suppressed at trial by means of the exclusionary rule. Beyond the criminal trial context, injunctive relief or damages might also be available. In this Section, I will examine some applications of my approach.

[*166]

1. Subpoenas for Book Records or Search Query Data

Suppose the police suspect John Doe of murdering somebody with the use of an unusual poison. The police issue subpoenas to bookstores to find out whether Doe purchased any books on poison. They also subpoena his search queries from Google to see if he did any searches on poison. n286

The bookstore records clearly fall within the boundaries of the First Amendment because they concern the consumption of ideas. n287 Internet search queries are very similar to book records in that they involve a person's reading habits and intellectual pursuits. In Reno v. ACLU, n288 the Supreme Court likened the Internet to a "vast library including millions of readily available and indexed publications." n289 The content of the Internet, the Court noted, "is as diverse as human thought." n290

Having established that First Amendment activities are implicated, the court would turn to the question of whether the government activity will have a chilling effect on consumption of ideas. In this case, the police are seeking information for use in prosecuting Doe. Use in a criminal prosecution, under my approach, will almost always cause a chilling effect. In this case, use of the information in a criminal prosecution penalizes Doe for his reading and Internet searching. Therefore, the First Amendment would regulate the government's gathering of the information. n291 If the evidence were used at Doe's criminal trial, Doe could suppress it because it was obtained via an ordinary subpoena without requiring probable cause. n292 If he had notice of the subpoena, Doe could seek to quash it before its execution **[*167]** if the police were unable to demonstrate probable cause. In short, the First Amendment would require that the police seek prior judicial approval and show probable cause before requesting the data.

2. Obtaining ISP Records of an Anonymous Speaker

Suppose the FBI is investigating an organization for providing "material support" to terrorists. n293 FBI agents come across an anonymous blog where the blogger declares that he is a member of the organization, expresses how much he supports the organization's values, and urges others to join the group. The FBI obtains the IP address of the blogger and issues a National Security Letter (NSL) to the blogger's ISP to find out his identity. An NSL works similarly to a

subpoena, although its use often involves even fewer protections. n294 With an NSL, the FBI can compel ISPs and telephone companies to reveal customer records if they are "relevant" to a terrorism or intelligence investigation. n295

The use of the NSL would trigger First Amendment protections. The information sought pertains to the blogger's anonymous speech and the political groups with which he associates, so First Amendment values are implicated. n296 The blogger's political expression may be substantially chilled by the government's actions. Even if the evidence was not used in a criminal case against the blogger, the mere exposure of the blogger's identity to the government could have significant chilling effects. Given the blogger's radical and unpopular **[*168]** beliefs, she might be speaking anonymously precisely in order to shield her identity from the government.

Some might contend that the NSL's built-in safeguards for First Amendment activity are sufficient to satisfy the First Amendment's demands. Most NSL provisions, including the one for ISP records, require that the FBI certify that the records are "relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities, provided that such an investigation of a United States person is not conducted solely on the basis of activities protected by the First Amendment to the Constitution of the United States." n297 This provision, however, is far too narrow. Hardly any investigations are conducted "solely" on the basis of First Amendment activities. Law enforcement officials will invariably argue that their investigation is based at least in some part on criminal activity. The focus of the inquiry should not be on whether the investigations are targeted exclusively to First Amendment activities but on whether the investigations have a chilling effect on such activities. Therefore, the First Amendment provisions of the NSL are not sufficiently protective of First Amendment rights, and the warrant requirement would apply.

3. Collecting Phone Call Records

In Smith v. Maryland, n298 the Supreme Court held that the Fourth Amendment does not apply to pen register data. n299 Accordingly, lists of phone numbers that people dial and logs of the numbers of incoming calls are not protected by the Fourth Amendment, although they are given minimal statutory protection. n300 The USA PATRIOT Act extends this same minimal protection to e-mail headers and routing information (such as IP addresses). n301 Whether this minimal protection is sufficient to comply with the Constitution is an open question since the Court has not addressed whether Smith v. **[*169]** Maryland applies to e-mail headers or IP addresses, though such an interpretation is arguably possible. n302

Although the Supreme Court has focused on the Fourth Amendment, obtaining pen register data without a warrant potentially violates the First Amendment. A log of incoming and outgoing calls can be used to trace channels of communication. It is relatively easy to link a phone number to a person or organization. Pen registers can reveal associational ties, since association in contemporary times often occurs by way of telephone or e-mail. As David Cole argues, modern communications technology has made association possible without physical assembly. n303 For example, if the government scrutinized the phone logs of the main office of the Communist Party, it might discover many of the Party's members. The information would not be equivalent to a membership list, but it would probably include identifying data about countless individuals who would not want the government to discover their connection to the Communist Party. If the government were to examine the phone logs or e-mail headers of a particular individual, it might discover that the individual contacted particular organizations that the individual wants to keep private. The pen register information, therefore, implicates First Amendment values.

To make the First Amendment analysis more concrete, consider the following hypothetical case: A domestic political group known as the Terrorist Sympathizers Association seeks to demonstrate that although violent means are wrongheaded, the underlying political causes of terrorists have merit. The FBI suspects that a few members might be providing assistance to terrorists, and it wants to identify the group's members so it can investigate them more thoroughly. Under the very lax standard of the Pen Register Act, the government certifies that "the information likely to be obtained by such installation and use [of a pen register] is relevant to an ongoing criminal investigation." n304 With the pen register order, it obtains from the phone company a log of all the incoming and outgoing calls to the group's office so it can identify the individuals who have been in contact with the group.

[*170] In this hypothetical, association with the group would fall within the boundaries of the First Amendment because it is association "for the purpose of engaging in those activities protected by the First Amendment - speech, assembly, petition for the redress of grievances, and the exercise of religion." n305 The association here is for the "pursuit of a wide variety of political, social, economic, educational, religious, and cultural ends." n306

As for chilling effect, this is a criminal investigation for the potential purpose of prosecuting some of the group's members. People will likely be chilled from associating with the group if they are identified as members. The First Amendment would require a warrant supported by probable cause to obtain the phone logs.

Suppose instead that the NSA wants to obtain the phone call logs of everybody in the United States so that it can feed the data into its computers to determine who has called phone numbers associated with known terrorists or terrorist organizations. It is unclear how the government intends to use the information, and therefore it is difficult to demonstrate that the data collection will create a chilling effect. If the information were used to prosecute individuals, this would clearly chill some telephone communications. But in the hypothetical posed, the NSA is merely planning to analyze the data. It may use it for myriad purposes, most likely to identify individuals who should be subject to additional scrutiny. People will not know whether they have been so identified. Nevertheless, people might avoid calling certain groups for fear that they will wind up on a watch list or suspicious persons list. The problem is that the consequences in this case are unclear, as the government has not yet indicated what precisely it intends to do with the information. Under existing doctrine, establishing a chilling effect would likely be difficult.

In this case, overbreadth doctrine might provide the appropriate protection. Without more information about what groups the government is targeting, it is hard for any individual or group to bring a direct challenge to the information gathering. Any given person might have no idea whether the government is analyzing her associations or what precisely the government is doing with the data. Because the NSA's information gathering program is extremely broad and could capture a wide range of associational activity, an individual could bring an overbreadth challenge without being required to show that he personally has been chilled.

[*171]

4. Obtaining Financial Records

In United States v. Miller, n307 which established the third-party doctrine, the Court concluded that the Fourth Amendment did not apply to the subpoena at issue because individuals have no reasonable expectation of privacy in financial records held by financial institutions. n308 In a footnote, the Court explicitly left open the question of whether the First Amendment might limit subpoenas for financial records, noting that the respondent did "not contend that the subpoenas infringed upon his First Amendment rights." n309 Moreover, the Court noted that "there was no blanket reporting requirement ... nor any allegation of an improper inquiry into protected associational activities." n310

To what extent should the First Amendment protect financial records? Although financial records can reveal much activity that falls outside the scope of the First Amendment - such as fraud, conspiracy, embezzlement, money laundering, and other crimes - they can also reveal political associations. A few years before Miller, when the Supreme Court decided California Bankers Ass'n v. Shultz, n311 many Justices recognized that disclosure of bank records to the government might implicate freedom of association. Shultz involved a blanket reporting requirement, under the Bank Secrecy Act of 1970, which compels banks to provide information about people's financial transactions to the government. n312 A group of bankers and a group of account holders challenged the constitutionality of the Bank Secrecy Act. The primary purpose of the Act was to make it easier to detect fraud and other forms of white collar crime. n313 Under regulations to implement the Act, all international transactions exceeding $ 5000, n314 as well as domestic transactions exceeding $ 10,000, n315 had to be reported to the government. The Court held that the bankers did not have Fourth Amendment rights in the data because "corporations can claim no equality with individuals in the enjoyment of a right to privacy." n316 **[*172]** The account holders failed to allege that they engaged in transactions exceeding $ 10,000, and as a result, lacked standing. n317 The Court further rejected a Fifth Amendment challenge,

concluding that the bankers lacked "standing to assert Fifth Amendment claims on behalf of customers in general" and that the account holders failed to allege that "any of the information required by the Secretary will tend to incriminate them." n318

The Court also addressed a First Amendment challenge by the ACLU, which claimed that the reporting requirements infringed upon its right to freedom of association. n319 However, the Court found that the ACLU failed to allege that it engaged in the kinds of financial transactions that would be subject to reporting and therefore lacked standing. n320

Nonetheless, concurring and dissenting opinions noted that reporting requirements could infringe on First Amendment freedoms. In a concurrence, Justices Powell and Blackmun observed that the scope of the Act was limited by the reporting requirements, which only required reporting of transactions over particular amounts. n321 They then noted, however, that "[a] significant extension of the regulations' reporting requirements ... would pose substantial and difficult constitutional questions ... . Financial transactions can reveal much about a person's activities, associations, and beliefs." n322 Justice Douglas in dissent argued that "banking transactions of an individual give a fairly accurate account of his religion, ideology, opinions, and interests." n323 Justices Brennan and Marshall also noted that First Amendment rights were potentially implicated. n324 Thus in both Miller and Shultz, several Justices acknowledged that First Amendment activities could be implicated by the collection of financial records, but the Court nonetheless managed to avoid squarely addressing the issue.

If the issue were properly before the Court, would the First Amendment be implicated? Suppose the government were to subpoena **[*173]** the bank account records of the hypothetical Terrorist Sympathizers Association, discussed earlier, because it suspects that the group might be furnishing financial assistance to terrorists and wants to investigate contributors to the group. This investigation would be an "inquiry into protected associational activities" that fall within the boundaries of the First Amendment. n325 Providing donations is an essential part of freedom of association. As the Court noted in Buckley v. Valeo, n326 "The right to join together 'for the advancement of beliefs and ideas' ... is diluted if it does not include the right to pool money through contributions, for funds are often essential if advocacy is to be truly or optimally effective." n327 As David Cole argues, "Groups cannot exist without the material support of their members and associates. If the right of association meant only that one had the right to join organizations but not to support them, the right would be empty." n328 The government's criminal investigation could ultimately have a chilling effect and inhibit people from donating money to controversial groups.

In several cases, federal circuit courts have held that subpoenas to banks for the account records of political groups trigger First Amendment scrutiny. n329 For example, in First National Bank v. United States, n330 the court held that a grand jury subpoena for bank account records of antitaxation groups implicated the First Amendment because "the constitutionally protected right, freedom to associate freely and anonymously, will be chilled equally whether the associational information is compelled from the organization itself or from third parties." n331 Because the activities affected fall within the boundaries of the First Amendment and a chilling effect is likely, I would argue that the First Amendment should regulate the government investigation of the Terrorist Sympathizers Association.

[*174] Suppose instead that the government subpoenaed the bank records of John Doe, whom it suspected of engaging in money laundering for a drug cartel. Criminal liability for money laundering is disconnected from Doe's political associations. Although the information gathering has the potential to cause some chilling, the limited purpose and scope of the investigation minimize the likelihood of a chilling effect on the exercise of First Amendment rights. In contrast, the Terrorist Sympathizers Association example involves potential criminal liability in connection with the expressive associational activities of that group.

A final question worth examining is whether the Bank Secrecy Act of 1970 is constitutional under the First Amendment. Its purpose is to gather evidence about criminal activity, so it does not appear to be directed toward First Amendment activities. Its effect, however, poses a risk of chilling many legitimate financial transactions involving political groups. Because of its great breadth and lack of procedures to prevent the government from using it to ferret

out information about group membership, the Act presents a much greater threat of chilling effect than a targeted inquiry would.

A finding that the First Amendment applies would not necessarily invalidate the Act. Instead, one would analyze whether the government interest justifying the Bank Secrecy Act is substantial and whether the Act is appropriately tailored to achieve that government interest. Ferreting out crime would clearly be a substantial government interest. The Court would then look to whether the law does so in an appropriately tailored manner so as not to unduly compromise First Amendment freedoms. I believe that this analysis as applied to the Bank Secrecy Act would be a difficult and contestable one. It would examine whether the government could achieve its goals with more narrowly tailored means. Such an analysis involves matters of white collar criminal investigation that are beyond the scope of this Article, but it is worth noting that such an analysis can and should take place.

An individual might also attack the Bank Secrecy Act under the overbreadth prong of my analysis. As Justice Douglas noted in dissent in Shultz, "making [financial transactions] automatically available to all federal investigative agencies is a sledge-hammer approach to a problem that only a delicate scalpel can manage." n332 While the Act might further substantial government interests in detecting unlawful financial activity, it also sweeps in a significant amount of lawful financial **[*175]** activity that is related to expressive associations. The Act might therefore be overbroad under the First Amendment.

5. Questioning a Person's Friends

Suppose the police are investigating John Doe for a hate crime. They interview Doe's friends to find out if he said anything to them about his attitudes toward minorities. Such interviews might indeed have a chilling effect on Doe's associational activities. However, even if the First Amendment were implicated, a warrant with probable cause would be too stringent a standard. Requiring a warrant with probable cause for instances when people talk voluntarily to government officials would restrict a large range of investigative activity. Under Fourth Amendment law, there are exceptions to the warrant and probable cause requirements when they are impractical. n333 In these cases, the courts engage in a general balancing, weighing the invasiveness of a particular government practice against the government's need for the information. n334

A rule requiring a warrant whenever law enforcement officials spoke to a person about a suspect would be extremely cumbersome. Police could not talk to witnesses of crimes - or even victims - without first getting a warrant. The voluntary nature of the dialogue between the government and the individuals makes the information gathering much less problematic than coerced forms of information gathering, such as subpoenas or National Security Letters or even surveillance. The First Amendment would simply require that the information gathering be voluntary. Gathering information from other individuals who voluntarily supply it would be sufficiently narrowly tailored to achieve the government's significant interest in investigating a crime. Such an approach is not perfect, as there may be some instances where people's conversations with others will be chilled. But a rule requiring a warrant with probable cause whenever the government speaks to a person about conversations with another would simply be too impractical, making many law enforcement investigations impossible without providing substantial benefits in terms of First Amendment protection.

If instead of seeking information voluntarily, the government were to issue a subpoena compelling witnesses to testify about **[*176]** another person's First Amendment activity, the First Amendment would require a higher procedural threshold, such as a warrant with probable cause or a subpoena with heightened standards (perhaps probable cause rather than relevance).

Conclusion

For far too long, courts and commentators have viewed the First Amendment as irrelevant to criminal procedure. But as Fourth and Fifth Amendment protections recede from those areas where First Amendment activity is most likely to

occur, it is time to look to the First Amendment for protection. Perhaps more so than any other amendment in the Bill of Rights, the First Amendment has iconic status, and it has grown massively in power and scope over the past century. Unlike the Fourth and Fifth Amendments, the First Amendment shows no sign of weakening. In this Article, I have demonstrated that First Amendment criminal procedure is both justified and necessary to prevent the infringement of First Amendment rights in the course of government investigations. It is time for the First Amendment to take its place alongside the Fourth and Fifth Amendments as a source of constitutional criminal procedure.

Legal Topics:

For related research and practice materials, see the following legal topics:
Computer & Internet LawCriminal OffensesSearch & SeizureConstitutional LawBill of RightsFundamental FreedomsFreedom of ReligionFree Exercise of ReligionConstitutional LawBill of RightsFundamental FreedomsFreedom of SpeechScope of Freedom

FOOTNOTES:

n1. The First Amendment provides: "Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances." U.S. Const. amend. I.

n2. See Fisher v. United States, 425 U.S. 391, 397 (1976) (holding that use of subpoena to obtain records from third party does not violate Fifth Amendment privilege of person under investigation); United States v. Dionisio, 410 U.S. 1, 9 (1973) (holding that subpoenas are not searches under Fourth Amendment).

n3. See generally Daniel J. Solove, The Digital Person: Technology and Privacy in the Information Age 202-03 (2004) (describing subpoenas and contrasting them with warrants).

n4. United States v. Miller, 425 U.S. 435, 443 (1976).

n5. Saul Hansell, Online Trail Can Lead to Court, N.Y. Times, Feb. 4, 2006, at C1.

n6. Bob Tedeschi, Patriot Act Has Led Online Buyers and Sellers to Watch What They Do. Could It Threaten Internet Business?, N.Y. Times, Oct. 13, 2003, at C6.

n7. Felicity Barringer, Using Books as Evidence Against Their Readers, N.Y. Times, Apr. 8, 2001, at 4.3.

n8. Jeffrey Rosen, The Unwanted Gaze 31-33 (2000).

n9. See David A. Anderson, Freedom of the Press, 80 Tex. L. Rev. 429, 434-35 (2002) (noting that what constitutes "the press" for constitutional purposes is called into question by blogging).

n10. USA PATRIOT Act §215, 115 Stat. 287 (2001) (codified as amended at 50 U.S.C. §1861 (Supp. III 2005)).

n11. See Leslie Cauley, NSA Has Massive Database of Americans' Phone Calls, USA Today, May 11, 2006, at A1 (reporting on NSA program to collect millions of call records from telephone companies and noting that while NSA wiretapping authority is limited to international calls, acquisition of phone records may facilitate broad access to personal information about domestic callers). While the details of the NSA surveillance and information gathering programs are still shrouded in secrecy, it seems clear that the information gathered by the NSA relates to communication and association. See Seymour M. Hersh, Listening In, New Yorker, May 2006, at 25 (describing, in conjunction with NSA surveillance and information gathering programs, NSA's "chaining" process that begins with suspect phone number and then expands outward through several "levels of separation" to observe calling patterns of persons associated with suspect number).

n12. Linda E. Fisher, Guilt by Expressive Association: Political Profiling, Surveillance and the Privacy of Groups, 46 Ariz. L. Rev. 621, 625-26 (2004).

n13. U.S. Gen. Accounting Office, Data Mining: Federal Efforts Cover a Wide Range of Uses 1-3 (2004) (discussing various government data mining endeavors); Daniel J. Solove, Marc Rotenberg & Paul M. Schwartz, Information Privacy Law 604-17 (2d ed. 2006) (describing government data mining programs).

n14. See infra Part I.

n15. The Fourth Amendment provides that people shall "be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures" and that "no Warrants shall issue, but upon probable cause,

supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." U.S. Const. amend. IV.

n16. 389 U.S. 347 (1967).

n17. Id. at 361 (Harlan, J., concurring).

n18. See Winston v. Lee, 470 U.S. 753, 759 (1985) (noting general rule that when probable cause is present "a search is generally 'reasonable'" for purposes of Fourth Amendment).

n19. Brinegar v. United States, 338 U.S. 160, 175-76 (1949) (internal quotation marks omitted).

n20. Mapp v. Ohio, 367 U.S. 643, 655 (1961).

n21. U.S. Const. amend. V.

n22. The information must be compelled; it must involve testimony (not documents and things); and it must be incriminating. See, e.g., Schmerber v. California, 384 U.S. 757, 761 & n.5 (1966) (upholding use of compulsory blood test because Fifth Amendment "protects an accused only from being compelled to testify against himself, or otherwise provide the State with evidence of a testimonial or communicative nature").

n23. Mincey v. Arizona, 437 U.S. 385, 398 (1978); Ziang Sung Wan v. United States, 266 U.S. 1, 14 (1924).

n24. U.S. Const. amend. I.

n25. Sable Commc'ns of Cal., Inc. v. FCC, 492 U.S. 115, 126 (1989).

n26. Perry Educ. Ass'n v. Perry Local Educators' Ass'n, 460 U.S. 37, 45 (1983).

n27. See Robert L. Tsai, Speech and Strife, 67 Law & Contemp. Probs. 83, 86 (2004) ("The right to free speech remains the most cherished and recognizable right ... .").

n28. John Milton, Areopagitica (1644), reprinted in Areopagitica and Other Prose Writings 58 (William Haller, ed., MacMillan 1927).

n29. See Martin H. Redish, The Value of Free Speech, 130 U. Pa. L. Rev. 591, 593 (1982) ("Free speech ultimately serves only one true value, which I have labeled 'individual self-realization.'"); David A.J. Richards, Free Speech and Obscenity Law: Toward a Moral Theory of the First Amendment, 123 U. Pa. L. Rev. 45, 62 (1975) ("The value of free expression ... rests on its deep relation to self-respect arising from autonomous self-determination...."); David A. Strauss, Persuasion, Autonomy, and Freedom of Expression, 91 Colum. L. Rev. 334, 353-60 (1991) (presenting autonomy as justification for principle that speech cannot be restricted solely on grounds of its persuasiveness).

n30. See Owen M. Fiss, The Irony of Free Speech 3 (1996) ("Speech is valued so importantly in the Constitution ... not because it is a form of self-expression or self-actualization but rather because it is essential for collective self-determination."); Alexander Meiklejohn, Political Freedom 26 (1960) (contending that First Amendment exists to protect political deliberation); Cass R. Sunstein, Free Speech Now, 59 U. Chi. L. Rev. 255, 301 (1992) ("The First Amendment is principally about political deliberation.").

n31. Whitney v. California, 274 U.S. 357, 375 (1927).

n32. Palko v. Connecticut, 302 U.S. 319, 327 (1937).

n33. 319 U.S. 624 (1943).

n34. Id. at 642.

n35. Vincent Blasi & Seana V. Shiffrin, The Story of West Virginia State Board of Education v. Barnette: The Pledge of Allegiance and the Freedom of Thought, in Constitutional Law Stories 433, 457 (Michael C. Dorf ed., 2004).

n36. Id. at 461.

n37. See Paul M. Schwartz, Privacy and Democracy in Cyberspace, 52 Vand. L. Rev. 1609, 1653 (1999) ("The health of a democratic society depends both on the group-oriented process of democratic deliberation and the functioning of each person's capacity for self-governance.").

n38. Talley v. California, 362 U.S. 60, 64 (1960).

n39. Id. at 65.

n40. Robert D. Putnam, Bowling Alone: The Collapse and Revival of American Community 173 (2000); see also C. Keith Boone, Privacy and Community, 9 Soc. Theory & Prac. 1, 8 (1983) ("Privacy seems vital to a democratic society [because] ... it underwrites the freedom to vote, to hold political discussions, and to associate freely away from the glare of the public eye and without fear of reprisal.").

n41. See Meiklejohn, supra note 30, at 24 (describing "the traditional American town meeting" as "a model by which free political procedures may be measured").

n42. See infra Part II.B.3.

n43. Julie E. Cohen, A Right to Read Anonymously: A Closer Look at "Copyright Management" in Cyberspace, 28 Conn. L. Rev. 981, 1006 (1996) ("Thoughts and opinions, which are the predicates to speech,

cannot arise in a vacuum. Whatever their content, they are responses formed to things heard or read.").

n44. Marc Jonathan Blitz, Constitutional Safeguards for Silent Experiments in Living: Libraries, the Right to Read, and a First Amendment Theory for an Unaccompanied Right to Receive Information, 74 UMKC L. Rev. 799, 803 (2006).

n45. Id. at 802-03.

n46. 1 Alexis de Tocqueville, Democracy in America 196 (Vintage Books 1990) (1835).

n47. NAACP v. Alabama ex rel. Patterson, 357 U.S. 449, 462 (1958).

n48. See Jerry Kang, Information Privacy in Cyberspace Transactions, 50 Stan. L. Rev. 1193, 1260 (1998) ("Simply put, surveillance leads to self-censorship."); see also Julie E. Cohen, Examined Lives: Informational Privacy and the Subject as Object, 52 Stan. L. Rev. 1373, 1426 (2000) (arguing that surveillance results in "a subtle yet fundamental shift in the content of our character, a blunting and blurring of rough edges and sharp lines"); Christopher Slobogin, Public Privacy: Camera Surveillance of Public Places and the Right to Anonymity, 72 Miss. L.J. 213, 242-47 (2002) (arguing that exposure to surveillance alters people's behavior, causing them to become more cautious in their actions).

n49. See, e.g., Schwartz, supra note 37, at 1648-59 (arguing that lack of adequate privacy protection on Internet undermines its potential as forum for deliberative democracy, which depends on capacity for individual self-determination online).

n50. See Kyllo v. United States, 533 U.S. 27, 31 (2001) ("With few exceptions, the question whether a warrantless search of a home is reasonable and hence constitutional must be answered no.").

n51. Fed. R. Crim. P. 17(c)(1).

n52. Fed. R. Crim. P. 17(a) ("The clerk must issue a blank subpoena - signed and sealed - to the party requesting it, and that party must fill in the blanks before the subpoena is served."); In re Subpoena Duces Tecum, 228 F.3d 341, 347-48 (4th Cir. 2000) ("While the Fourth Amendment protects people against unreasonable searches and seizures, it imposes a probable cause requirement only on the issuance of warrants. Thus, unless subpoenas are warrants, they are limited by the general reasonableness standard of the Fourth Amendment[,] ... not by the probable cause requirement." (internal quotation marks and citation omitted)); Baylson v. Disciplinary Bd. of Supreme Court of Pa., 975 F.2d 102, 106 (3d Cir. 1992) ("Specifically, Fed.R.Crim.P. 17 provides in relevant part that the clerk of the court, without judicial supervision, shall issue a subpoena to a party requesting it.").

n53. A subpoena will be quashed on relevancy grounds if "there is no reasonable possibility that the category of materials the Government seeks will produce information relevant to the general subject of the grand jury's investigation." United States v. R. Enters., Inc., 498 U.S. 292, 301 (1991).

n54. William J. Stuntz, O.J. Simpson, Bill Clinton, and the Transsubstantive Fourth Amendment, 114 Harv. L. Rev. 842, 857-58 (2001).

n55. 410 U.S. 1 (1973).

n56. Id. at 8. The Court was nonetheless not prepared to conclude that subpoenas always fall outside the Fourth Amendment, stating that "the Fourth Amendment provides protection against a grand jury subpoena duces tecum too sweeping in its terms 'to be regarded as reasonable.'" Id. at 11 (quoting Hale v. Henkel, 201 U.S. 43, 76 (1906)).

n57. Fisher v. United States, 425 U.S. 391, 410 (1976).

n58. Christopher Slobogin, Subpoenas and Privacy, 54 DePaul L. Rev. 805, 822 (2005).

n59. 409 U.S. 322, 329 (1973) (subpoena to individual's accountant for his documents did not violate Fifth Amendment).

n60. Fisher, 425 U.S. at 410-11 (1976) (holding that subpoena for documents in possession of attorney for party being investigated did not violate Fifth Amendment); see also Andresen v. Maryland, 427 U.S. 463, 477 (1976) (holding that gathering information already in existence and voluntarily committed to writing did not violate Fifth Amendment).

n61. 425 U.S. 435 (1976).

n62. Id. at 443.

n63. 442 U.S. 735 (1979).

n64. Id. at 743.

n65. Id. at 745-46. "A pen register is a device that is typically installed at the telephone company's offices that can record the telephone numbers a person dials." Daniel J. Solove, Digital Dossiers and the Dissipation of Fourth Amendment Privacy, 75 S. Cal. L. Rev. 1083, 1134 n.306 (2002).

n66. 55 F. Supp. 2d 504 (W.D. Va. 1999).

n67. Id. at 508.

n68. 81 F. Supp. 2d 1103 (D. Kan. 2000).

n69. Id. at 1110.

n70. 255 F.3d 325 (6th Cir. 2001).

n71. Id. at 336.

n72. See Solove, supra note 3, at 165-75.

n73. See California v. Greenwood, 486 U.S. 35, 39-40 (1988) (holding that individuals lack reasonable expectation of privacy in garbage left for collection because it will be conveyed "to a third party, the trash collector").

n74. Robbins v. California, 453 U.S. 420, 425-26 (1981). Not all searches of containers require a warrant, such as containers in automobiles. See United States v. Ross, 456 U.S. 798, 822-23 (1982) ("As Justice Stewart stated in Robbins, the Fourth Amendment provides protection to the owner of every container that conceals its contents from plain view. But the protection afforded by the Amendment varies in different settings." (internal citation omitted)).

n75. Harris v. United States, 390 U.S. 234, 236 (1968).

n76. See Florida v. Riley, 488 U.S. 445, 448-50 (1989) (holding that aerial surveillance of greenhouse interior with roof panels missing was not covered by Fourth Amendment as observed activity was visible to public from sky); see also Slobogin, supra note 48, at 233 ("Meaningful legal strictures on government use of public surveillance cameras in Great Britain, Canada, and the United States are non-existent.").

n77. See, e.g., Lewis v. United States, 385 U.S. 206, 210-11, 213 (1966) (holding that Fourth Amendment did not apply when defendant invited undercover agent into his home to engage in illegal sale of narcotics).

n78. 385 U.S. 293 (1966).

n79. Id. at 302.

n80. Id.

n81. See, e.g., United States v. White, 401 U.S. 745, 751 (1971) (holding that Fourth Amendment does not protect information conveyed to government informant who wears radio transmitter); On Lee v. United States, 343 U.S. 747, 753-54 (1952) (concluding that Fourth Amendment does not apply when person misplaces trust by talking to bugged government informant).

n82. Occasionally, in dissents and dicta, Justices have mentioned how government investigations can implicate First Amendment rights. See, e.g., United States v. U.S. Dist. Court, 407 U.S. 297, 314 (1972) ("Fourth Amendment protections become the more necessary when the targets of official surveillance may be those suspected of unorthodoxy in their political beliefs."); White, 401 U.S. at 762 (Douglas, J., dissenting) ("Monitoring, if prevalent, certainly kills free discourse and spontaneous utterances. Free discourse - a First Amendment value ... is not free if there is surveillance."); Lopez v. United States, 373 U.S. 427, 470 (1963) (Brennan, J., dissenting) (noting that "historically the search and seizure power was used to suppress freedom of speech and of the press" and that "freedom of speech is undermined where people fear to speak unconstrainedly in what they suppose to be the privacy of home and office").

n83. 367 U.S. 717 (1961).

n84. See id. at 731-32.

n85. Id. at 724.

n86. 378 U.S. 205 (1964).

n87. Id. at 211-12.

n88. 379 U.S. 476 (1965).

n89. Tex. Rev. Civ. Stat. Ann. art. 6889-3A, §2 (Vernon 1957) (repealed 1993).

n90. Stanford, 379 U.S. at 480.

n91. Id. at 485 (emphasis added) (internal citations omitted). In Lee Art Theatre, Inc. v. Virginia, 392 U.S. 636 (1968), the Court appeared to reaffirm the rule of Marcus and Stanford when it invalidated a warrant to seize obscene films because the evidentiary support offered for it "fell short of constitutional requirements demanding necessary sensitivity to freedom of expression." Id. at 637.

n92. 413 U.S. 496 (1973).

n93. Id. at 504.

n94. 436 U.S. 547, 550-51 (1978).

n95. Id. at 554.

n96. Id. at 563.

n97. Id. at 565.

n98. Id. Congress responded to the problem in the Zurcher case with the Privacy Protection Act, which prevents government officers from collecting documents from "a person reasonably believed to have a purpose to disseminate to the public a newspaper, book, broadcast, or other similar form of public communication." 42 U.S.C. §2000aa(a) (2000).

n99. New York v. P.J. Video, Inc., 475 U.S. 868, 873-74 (1986) (internal quotation marks omitted); see also Maryland v. Macon, 472 U.S. 463, 470 (1985) (holding that police officer merely purchasing book does not implicate Fourth or First Amendment). But cf. Fort Wayne Books, Inc. v. Indiana, 489 U.S. 46, 63 (1989) (holding that where allegedly obscene films or books are seized for purposes of destroying them or blocking their distribution, as opposed to seizing single copy to preserve evidence of criminal undertaking, probable cause alone is insufficient to justify seizure).

n100. See Schmerber v. California, 384 U.S. 757, 767 (1966) ("The overriding function of the Fourth Amendment is to protect personal privacy and dignity against unwarranted intrusion by the State.").

n101. Akhil Reed Amar, Fourth Amendment First Principles, 107 Harv. L. Rev. 757, 806 (1994).

n102. Zurcher, 436 U.S. at 564 (quoting Roaden v. Kentucky, 413 U.S. 496, 501 (1973)).

n103. The scholars I discuss in this Section have many significant disagreements over the historical background of the First, Fourth, and Fifth Amendments. Rather than address these disagreements, I have focused on certain dimensions of the history relevant to this Article. For more background on these debates, see Morgan Cloud, Searching Through History; Searching for History, 63 U. Chi. L. Rev. 1707 (1996) (reviewing William J. Cuddihy, The Fourth Amendment: Origins and Original Meaning, 602-1791 (1990) (unpublished Ph.D. dissertation, Claremont Graduate School) (on file with the New York University Law Review)).

n104. Akhil Reed Amar, The Bill of Rights as a Constitution, 100 Yale L.J. 1131, 1201 (1991).

n105. Id. at 1131.

n106. See, e.g., Marcus v. Search Warrant, 367 U.S. 717, 729 (1961) ("The Bill of Rights was fashioned against the background of knowledge that unrestricted power of search and seizure could also be an instrument for stifling liberty of expression.").

n107. William J. Stuntz, The Substantive Origins of Criminal Procedure, 105 Yale L.J. 393, 395 (1995).

n108. Larry D. Eldridge, Before Zenger: Truth and Seditious Speech in Colonial America, 1607-1700, 39 Am. J. Legal Hist. 337, 337 (1995).

n109. See Thomas K. Clancy, The Fourth Amendment's Concept of Reasonableness, 2004 Utah L. Rev. 977, 1035 & n.364 ("There is strong historical support for the protection of 'papers,' that is, materials related to free speech."); Sherry F. Colb, Innocence, Privacy, and Targeting in Fourth Amendment Jurisprudence, 96 Colum. L. Rev. 1456, 1499-1500 (1996) (arguing that First and Fourth Amendments were infused by same "spirit" of protecting dissent); Nadine Strossen, The Fourth Amendment in the Balance: Accurately Setting the Scales Through the Least Intrusive Alternative Analysis, 63 N.Y.U. L. Rev. 1173, 1241 (1988) ("Since colonial days, governmental search and seizure powers have been used to curb freedom of speech.").

n110. For a description of the Zenger trial, see 1 Rodney A. Smolla, Law of Defamation §1:28, at 1-24.1 to 1-26 (2d ed. 2000 & Supp. 2005).

n111. William R. Glendon, The Trial of John Peter Zenger, N.Y. St. B.J., Dec. 1996, at 48, 52.

n112. 19 Howell's State Trials 1153 (C.P. 1763), 98 Eng. Rep. 489 (K.B.).

n113. Stuntz, supra note 107, at 398. For more information on this case, see Telford Taylor, Two Studies in Constitutional Interpretation 29-35 (1969).

n114. Stuntz, supra note 107, at 398-99.

n115. See Cuddihy, supra note 103, at 651-52 ("To control the press and religious as well as political dissent, the secretaries of state maintained a steady barrage of general warrants until 1763.").

n116. Wilkes, 19 Howell's State Trials at 1167, 98 Eng. Rep. at 498.

n117. See Cuddihy, supra note 103, at 927-30 (noting that press accounts of Wilkes's trial allowed "stirring proclamations against general warrants [to] reach[] countless numbers of the literate").

n118. Id. at 942.

n119. See Amar, supra note 104, at 1177 ("John Wilkes, and the author of the opinion, Lord Chief Justice Pratt (soon to become Lord Camden), were folk heroes in the colonies.").

n120. Cuddihy, supra note 103, at 1106. In the year following the Wilkes case, the Boston Gazette and the Country Journal discussed the case in thirty-six different stories. Eric Schnapper, Unreasonable Searches and Seizures of Papers, 71 Va. L. Rev. 869, 876 n.38 (1985). "Reprints of Wilkes' Authentic Account of his arrest appeared at Boston, New York, and Philadelphia before 1763 was finished. In 1767, at least ten newspapers from Rhode island [sic] to South Carolina carried either Wilkes' recollections of The North Briton searches or comments on those recollections." Cuddihy, supra note 103, at 1105-06 (internal citations omitted).

n121. 19 Howell's State Trials 1029 (C.P. 1765), 95 Eng. Rep. 807 (K.B.).

n122. Entick, 19 Howell's State Trials at 1064.

n123. See Amar, supra note 104, at 1177 ("Pennsylvania residents named the town of Wilkes-Barre after the plaintiff; New Jersey and South Carolina each dedicated a city in Camden's honor.").

n124. Stuntz, supra note 107, at 402-03.

n125. Id. at 403.

n126. Id. at 395; see also Andrew E. Taslitz, Reconstructing the Fourth Amendment: A History of Search and Seizure, 1789-1868, at 18 (2006) ("The abusive searches and seizures that captured colonial Americans' attention frequently involved state efforts to suppress dissent."). A desire to protect expressive activity from government intrusion was only one of the many influences on the Fourth Amendment. See David E. Steinberg, An Original Misunderstanding: Akhil Amar and Fourth Amendment History, 42 San Diego L. Rev. 227, 255 (2005) ("The Fourth Amendment proscription against unreasonable searches originated with English laws that protected homes against breaking and entering by private citizens.").

n127. Katharine B. Hazlett, The Nineteenth Century Origins of the Fifth Amendment Privilege Against Self-Incrimination, 42 Am. J. Legal Hist. 235, 237 (1998).

n128. See generally Leonard W. Levy, Origins of the Fifth Amendment 43-82 (2d ed. 1986) (describing history of ex officio oaths).

n129. Letter from Charles I to the High Commission (Feb. 4, 1637), in Historical Collections; Consisting of State Papers, and Other Authentic Documents; Intended as Materials for an History of the United States of America 428 (Ebenezer Hazard ed., Books for Libraries Press 1969) (1792-94).

n130. Levy, supra note 128, at 273-82.

n131. John H. Langbein, The Historical Origins of the Privilege Against Self-Incrimination at Common Law, 92 Mich. L. Rev. 1047, 1047 (1994); see also Eben Moglen, Taking the Fifth: Reconsidering the Origins of the Constitutional Privilege Against Self-Incrimination, 92 Mich. L. Rev. 1086, 1118 (1994).

n132. 96 U.S. 727 (1878).

n133. Id. at 733.

n134. 116 U.S. 616 (1886).

n135. Stuntz, supra note 107, at 423.

n136. Boyd, 116 U.S. at 626.

n137. Id. at 626-27.

n138. Id. at 630.

n139. Id. at 633.

n140. See Morgan Cloud, The Fourth Amendment During the Lochner Era: Privacy, Property, and Liberty in Constitutional Theory, 48 Stan. L. Rev. 555, 592-93 (1996) ("Boyd's interpretive linkage of the Fourth Amendment with the Fifth Amendment privilege against self-incrimination suggested that papers could be treated differently from other tangible personal property.").

n141. See Warden v. Hayden, 387 U.S. 294, 301-10 (1967) (rejecting "mere evidence" rule of Boyd, which had held that under Fourth Amendment police could only seize instrumentalities or fruits of crime, but could not seize items, like papers at issue in Boyd, that had only evidentiary value). For further discussion of Warden and its limitation of Boyd, see Morgan Cloud, A Liberal House Divided: How the Warren Court Dismantled the Fourth Amendment, 3 Ohio St. J. Crim. L. 33, 55-58 (2005).

n142. See, e.g., Fisher v. United States, 425 U.S. 391, 409-11 (1976); Couch v. United States, 409 U.S. 322, 329 (1973).

n143. See United States v. Dionisio, 410 U.S. 1, 10 (1973).

n144. See supra Part I.C.

n145. See Fisher, supra note 12, at 623 (finding that from its founding until at least 1970s, "the FBI regularly conducted politically motivated surveillance, choosing targets based on their political or religious beliefs").

n146. Whitfield Diffie & Susan Landau, Privacy on the Line: The Politics of Wiretapping and Encryption 138 (1998).

n147. See Herbert N. Foerstel, Surveillance in the Stacks: The FBI's Library Awareness Program 4 (1991).

n148. Id. at 2-4; Ulrika Ekman Ault, Note, The FBI's Library Awareness Program: Is Big Brother Reading over Your Shoulder?, 65 N.Y.U. L. Rev. 1532, 1533-39 (1990).

n149. See Richard Gid Powers, Secrecy and Power: The Life of J. Edgar Hoover 321 (1987).

n150. Ellen Schrecker, Many Are the Crimes: McCarthyism in America 203 (1998).

n151. See id. at 207-08.

n152. See id. at 228.

n153. See Select Comm. to Study Governmental Operations, Final Report of the Select Committee to Study Governmental Operations with Respect to Intelligence Activities of the United States Senate, S. Rep. No. 94-755, at 10-12 (1976) [hereinafter Church Committee Report] (describing COINTELPRO counterintelligence tactics in detail and characterizing them as "indisputably degrading to a free society"); David Cunningham,

There's Something Happening Here: The New Left, The Klan, and FBI Counterintelligence 6-9 (2004) (describing COINTELPRO program and noting that it led to "thousands of actions" against suspected Communist Party members, as well as actions against many other civil rights organizations); Powers, supra note 149, at 338-39 (discussing origins of COINTELPRO and fact that it applied "wartime counterintelligence methods to domestic groups").

n154. David Cunningham provides a list of scores of targeted groups. Cunningham, supra note 153, at 273-84; see also David Cole & James X. Dempsey, Terrorism and the Constitution: Sacrificing Civil Liberties in the Name of National Security 6-7 (2002) ("At the peak of its efforts, the FBI was investigating all major protest movements, from civil rights activists to Vietnam war protestors to women's liberation advocates.").

n155. Cunningham, supra note 153, at 8-9.

n156. For more on the FBI's surveillance of Martin Luther King, Jr., see generally David J. Garrow, The FBI and Martin Luther King, Jr. (1981).

n157. See Garrow, supra note 156, at 101-50.

n158. Church Committee Report, supra note 153, at 5.

n159. Office of the Attorney Gen., U.S. Dep't of Justice, Domestic Security Investigation Guidelines (1976).

n160. William C. Banks & M.E. Bowman, Executive Authority for National Security Surveillance, 50 Am. U. L. Rev. 1, 69 (2000).

n161. See id. at 69-70 (stating that where old guidelines required "specific and articulable facts" before opening investigation, new guidelines required only "reasonable indication").

n162. Office of the Attorney Gen., U.S. Dep't of Justice, The Attorney General's Guidelines on General Crimes, Racketeering Enterprise and Terrorism Enterprise Investigations 21-22 (2002), available at http://www.usdoj.gov/olp/general crimes2.pdf.

n163. Id. at 22. For more background about the guidelines, see generally Daniel J. Solove, Reconstructing Electronic Surveillance Law, 72 Geo. Wash. L. Rev. 1264, 1296-98 (2004).

n164. See, e.g., Solove, supra note 3, at 168-75 (describing data mining and government requests for personal data from businesses); Laura K. Donohue, Anglo-American Privacy and Surveillance, 96 J. Crim. L. & Criminology 1059, 1144-52 (2006) (discussing government data mining programs); Cauley, supra note 11 (discussing NSA program to collect phone call records of millions of Americans without authorization under Foreign Intelligence Surveillance Act); Eric Lichtblau & James Risen, Bank Data Sifted in Secret by U.S. to Block Terror, N.Y. Times, June 23, 2006, at A1 (describing CIA program examining financial transactions).

n165. United States v. U.S. Dist. Court, 407 U.S. 297 (1972). This case has come to be known as Keith based on the name of the District Court Judge, Damon Keith.

n166. Id. at 313.

n167. See David Cole, The New McCarthyism: Repeating History in the War on Terrorism, 38 Harv. C.R.-C.L. L. Rev. 1, 6-7 (2003) [hereinafter Cole, New McCarthyism] (discussing chilling effect of guilt by association on Communist political activity in McCarthy era); David Cole, Secrecy, Guilt by Association, and the Terrorist Profile, 15 J.L. & Religion 267, 282-86 (2000-2001) (discussing guilt by association in terrorism-related cases).

n168. Cole, New McCarthyism, supra note 167, at 6.

n169. Laird v. Tatum, 408 U.S. 1, 12-13 (1972).

n170. See Frederick Schauer, Fear, Risk and the First Amendment: Unraveling the "Chilling Effect," 58 B.U. L. Rev. 685, 692-93 (1978) (finding chilling effect doctrine independently significant only for "indirect

governmental restrictions of protected expression").

n171. Id. at 693.

n172. 408 U.S. 1.

n173. Id. at 6.

n174. Id. at 11.

n175. Id. at 13-14.

n176. Id. at 13; see also Slobogin, supra note 48, at 253-55 (offering such analysis of Laird).

n177. See, e.g., Phila. Yearly Meeting of the Religious Soc'y of Friends v. Tate, 519 F.2d 1335, 1337 (3d Cir. 1975) (holding that Laird foreclosed finding "a constitutional violation on the basis of mere police photographing and data gathering at public meetings"); Donohoe v. Duling, 465 F.2d 196, 201-02 (4th Cir. 1972) (finding alleged chilling effect of police photography not cognizable on basis of Laird).

n178. For example, in Bee See Books Inc. v. Leary, 291 F. Supp. 622 (S.D.N.Y. 1968), uniformed police officers routinely were stationed in plaintiffs' bookstores, which sold some hard-core pornography. The court concluded that the officers' presence violated the First Amendment because evidence showed that it resulted in a considerable drop in book sales. Id. at 623-24, 626. In Presbyterian Church (U.S.A.) v. United States, 870 F.2d 518 (9th Cir. 1989), Immigration and Naturalization Service (INS) agents wearing bugging devices entered churches and recorded religious services. The INS argued that Laird controlled, but the court concluded that the church had established a cognizable First Amendment injury because it had alleged "a concrete, demonstrable decrease in attendance at those worship activities." Id. at 522.

n179. See, e.g., Handschu v. Special Servs. Div., 349 F. Supp. 766, 770-71 (S.D.N.Y. 1972) (noting that government informers infiltrating groups, urging members to engage in illegal activities, and keeping dossiers on members "would seem by far to exceed the passive observational activities" upheld in Laird); White v. Davis, 533 P.2d 222, 226-27, 229 (Cal. 1975) (distinguishing Laird and concluding that "as a practical matter, the presence in a university classroom of undercover officers taking notes to be preserved in police dossiers must inevitably inhibit the exercise of free speech both by professors and students"). But see Gordon v. Warren Consol. Bd. of Educ., 706 F.2d 778, 780-81 (6th Cir. 1983) (holding that undercover agents investigating drug trafficking in high school did not create chilling effect because "there is not a single allegation that the covert operation in and of itself resulted in tangible consequences").

n180. Phila. Yearly Meeting, 519 F.3d at 1338-39 (finding "immediately threatened injury to plaintiffs by way of a chilling of their rights to freedom of speech and associational privacy" when collected information was available to nonpolice parties and was disclosed on television); Alliance to End Repression v. Rochford, 407 F. Supp. 115, 116-17 (N.D. Ill. 1975) (holding that allegations of wiretapping, unlawful entry, and dissemination of information "differ greatly" from those in Laird).

n181. 362 U.S. 60 (1960).

n182. Id. at 64-65.

n183. Id.

n184. 514 U.S. 334, 357 (1995).

n185. Id. at 341-42; see also Watchtower Bible & Tract Soc'y of N.Y., Inc. v. Vill. of Stratton, 536 U.S. 150, 166 (2002) (quoting McIntyre, 514 U.S. at 341-42).

n186. Under the Stored Communications Act, the government can obtain customer records at ISPs by providing "specific and articulable facts showing that there are reasonable grounds to believe that ... the records or other information sought, are relevant and material to an ongoing criminal investigation." 18 U.S.C. §2703(c)(1)(B)-(C), (d) (2000).

n187. 140 F. Supp. 2d 1088 (W.D. Wash. 2001).

n188. Id. at 1093.

n189. See, e.g., Columbia Ins. Co. v. Seescandy.com, 185 F.R.D. 573, 578 (N.D. Cal. 1999) (finding "limiting principals [sic]" on discoverability of defendant's identity due to "legitimate and valuable right to participate in online forums anonymously"); Doe No. 1 v. Cahill, 884 A.2d 451, 457 (Del. 2005) (holding that, because of potential chilling effect of low standard, defamation plaintiffs must satisfy "summary judgement" standard to obtain anonymous defendant's identity); Dendrite Int'l, Inc. v. Doe, No. 3, 775 A.2d 756, 760-61 (N.J. Super. Ct. App. Div. 2001) (offering guidelines for balancing First Amendment right to anonymous speech against plaintiff's right to assert claims against actionable anonymous conduct).

n190. 394 U.S. 557 (1969).

n191. Id. at 564 (citation omitted).

n192. Cohen, supra note 43, at 1012; see also Blitz, supra note 44, at 800 ("It is now well established that the First Amendment protects not only the rights of people to engage in speech but also the right of audiences to receive it." (citing Stanley, 394 U.S. at 564)).

n193. 381 U.S. 301 (1965).

n194. Id. at 307.

n195. Id.

n196. In re Grand Jury Subpoenas Duces Tecum, 78 F.3d 1307, 1312 (8th Cir. 1996) ("A grand jury subpoena will be enforced despite a First Amendment challenge if the government can demonstrate a

compelling interest in ... the information sought ... ." (citation omitted)); A Grand Jury Witness v. United States (In re Grand Jury Proceedings), 776 F.2d 1099, 1102-03 (2d Cir. 1985) (noting "well established" standard that government interests must be "compelling" and "sufficiently important to outweigh the possibility of infringement" when grand jury subpoena implicates First Amendment rights (citations omitted)); Grandbouche v. United States (In re Grand Subpoena to First Nat'l Bank), 701 F.2d 115, 119 (10th Cir. 1983) (holding that if enforcement of subpoena will chill freedom of association, government "must show a compelling need to obtain documents identifying petitioners' members" (citation omitted)).

n197. 26 Media L. Rep. (BNA) 1599 (D.D.C. 1998).

n198. Id. at 1600 (quoting Kleindienst v. Mandel, 408 U.S. 753, 762 (1972)).

n199. Id. at 1601. The case was settled before the court engaged in the requisite First Amendment balancing.

n200. Roberts v. U.S. Jaycees, 468 U.S. 609, 618 (1984) (recognizing "expressive association" as distinct from "intimate association"); see also Hurley v. Irish-Am. Gay, Lesbian & Bisexual Group of Boston, Inc., 515 U.S. 557, 568-70 (1995) (finding marching in parade to be constitutionally protected expressive association).

n201. 357 U.S. 449 (1958).

n202. Id. at 460 (citations omitted).

n203. Id. at 462.

n204. Id.

n205. 361 U.S. 516, 523-24 (1960) (holding that disclosure of NAACP membership lists "would work a

significant interference with the freedom of association of their members" because of "uncontroverted" likelihood of ensuing "harassment and threats of bodily harm").

n206. 372 U.S. 539, 546 (1963) (finding that publicizing NAACP membership information during committee hearing would amount to "a substantial abridgment of associational freedom").

n207. 424 U.S. 1 (1976) (per curiam).

n208. Id. at 64.

n209. Id. at 68.

n210. 354 U.S. 234 (1957).

n211. Id. at 250.

n212. 364 U.S. 479 (1960).

n213. Id. at 480, 490.

n214. Id. at 490.

n215. Id. at 488.

n216. 401 U.S. 1 (1971).

n217. Id. at 5. "When a State attempts to make inquiries about a person's beliefs or associations, its power is limited by the First Amendment. Broad and sweeping state inquiries into these protected areas, as Arizona has engaged in here, discourage citizens from exercising rights protected by the Constitution." Id. at 6.

n218. See, e.g., Grandbouche v. United States (In re Grand Subpoena to First Nat'l Bank), 701 F.2d 115, 119 (10th Cir. 1983) (finding that First Amendment was implicated by grand jury subpoena to bank for account records of two antitaxation groups because "the constitutionally protected right, freedom to associate freely and anonymously, will be chilled equally whether the associational information is compelled from the organization itself or from third parties"); Local 1814 v. Waterfront Comm'n, 667 F.2d 267, 272 (2d Cir. 1981) (concluding that subpoena for list of contributors to political committee violated First Amendment because "compelled disclosure of the Fund's contributors under the circumstances of this case would give rise to a chilling effect similar to the one recognized by the Supreme Court in Shelton v. Tucker"); United States v. Citizens State Bank, 612 F.2d 1091, 1094 (8th Cir. 1980) (finding that antitax group's allegations that subpoena to bank for account records caused "adverse effects" on its "organizational and fundraising activities" established "prima facie showing of arguable First Amendment infringement"); Paton v. LaPrade, 524 F.2d 862, 865, 870 (3d Cir. 1975) (holding that "mail cover" - recording of information appearing on outside of envelopes - violated individual's First Amendment rights because "factfinder reasonably might conclude that the FBI investigation adversely affected Paton's standing in school and in her community").

n219. 408 U.S. 665 (1972).

n220. Id. at 682-83 ("The First Amendment does not invalidate every incidental burdening of the press that may result from the enforcement of civil or criminal statutes of general applicability.").

n221. Id. at 707-08.

n222. Id. at 709 (Powell, J., concurring).

n223. Id. at 710.

n224. Id.

n225. Subsequent decisions have done little to clarify the scope of the First Amendment privilege for journalists. C. Thomas Dienes, Lee Levine & Robert C. Lind, Newsgathering and the Law §16.06, at 930 (3d ed. 2005). In Herbert v. Lando, 441 U.S. 153 (1979), the Court held that in defamation cases, the First Amendment does not restrict plaintiffs from "inquiring into the editorial processes of those responsible for the publication." Id. at 155.

n226. Dienes et al., supra note 225, §16.07, at 948.

n227. Id. §16.07, at 948-50 (arguing that "majority approach" of lower courts is exemplified by Second Circuit, which has held that journalist's right to protect confidential sources can only be outweighed by overriding and compelling interest).

n228. See supra Part I.

n229. As David Cole notes, "The right of association is potentially limitless. Virtually everything we do in society involves some degree of association with someone else." David Cole, Hanging with the Wrong Crowd: Of Gangs, Terrorists, and the Right of Association, 1999 Sup. Ct. Rev. 203, 232.

n230. Frederick Schauer, The Boundaries of the First Amendment: A Preliminary Exploration of Constitutional Salience, 117 Harv. L. Rev. 1765, 1786 (2004).

n231. Id. at 1768.

n232. Id. at 1807.

n233. Robert Post, Recuperating First Amendment Doctrine, 47 Stan. L. Rev. 1249, 1255 (1995) ("First

Amendment analysis is relevant only when the values served by the First Amendment are implicated.").

n234. Id. at 1254.

n235. Id. at 1255.

n236. Miller v. California, 413 U.S. 15, 36-37 (1973) (holding that obscene material is not generally protected by First Amendment and can be regulated even absent demonstration that it is without redeeming social value). But see Stanley v. Georgia, 394 U.S. 557, 559 (1969) (holding that First Amendment prohibits states from criminalizing mere private possession of obscene material).

n237. Chaplinsky v. New Hampshire, 315 U.S. 568, 572 (1942). But see R.A.V. v. City of St. Paul, 505 U.S. 377, 383-84 (holding that First Amendment requires that restrictions on use of fighting words, as well as on other low-value speech, be viewpoint neutral).

n238. New York v. Ferber, 458 U.S. 747, 763-64 (1982).

n239. I am not defending as a normative matter the Court's existing doctrinal categorizations of speech and nonspeech; rather, I am merely pointing out that the Court has recognized that not every instance of communication and association falls within the scope of the First Amendment.

n240. 201 U.S. 43 (1906).

n241. See id. at 74. But cf. Slobogin, supra note 58, at 815-17 (noting that although many cases in first half of twentieth century, including Hale, allowed very low standard for subpoenas for business papers, Hale suggested that subpoenas for private records might require higher standard). According to William Stuntz, the Hale approach was a cheat, a way to "keep Boyd and Entick but cabin them with illogical boundaries, making the protection non-threatening (or at least non-fatal) to the emergence of the regulatory state." Stuntz, supra note 107, at 432. However, although the Court's boundaries do not follow strict logic, they are not entirely indefensible. After all, it is a fiction to call a corporation a "person," and once one fiction is created, other departures from a strictly logical approach might be needed to cabin the fiction within logical boundaries. In

other words, the fact that the Court held that a corporation should enjoy some of the rights that persons have under the Constitution does not require the Court to conclude that corporations should have all of those rights.

n242. Schauer, supra note 170, at 701.

n243. Jonathan R. Siegel, Note, Chilling Injuries as a Basis for Standing, 98 Yale L.J. 905, 916 (1989) ("Laird v. Tatum did not clarify the difference between objective and subjective chills, and the lower courts have not reached agreement on the meanings of these terms.").

n244. See N.Y. Times Co. v. Sullivan, 376 U.S. 254, 271-72 (1964) (arguing that although libel can be restricted under First Amendment, "breathing space" must be provided so as not to chill protected speech).

n245. See supra Part II.B.4.

n246. See supra Parts II.B.2-3.

n247. See supra Part II.B.1.

n248. 357 U.S. 449 (1958).

n249. Id. at 462-63.

n250. E.g., Baird v. State Bar of Ariz., 401 U.S. 1 (1971); Shelton v. Tucker, 364 U.S. 479 (1960).

n251. 380 U.S. 479 (1965).

n252. Id. at 487.

n253. Id. at 492-95 (striking down Louisiana's Subversive Activities and Communist Control Law, La. Rev. Stat. Ann. §§14:358-374 (Cum. Supp. 1962), which required members of "Communist Front Organizations" to register with authorities).

n254. Laird v. Tatum, 408 U.S. 1, 3, 6 (1972).

n255. This hypothetical is based on Maryland v. Macon, 472 U.S. 463 (1985), where the Court concluded that the mere purchase of a book by a law enforcement official does not implicate either the Fourth Amendment or the First. Id. at 468-70.

n256. NAACP v. Alabama ex rel. Flowers, 377 U.S. 288, 307 (1964).

n257. Thornhill v. Alabama, 310 U.S. 88, 98 (1940) (holding that after arrest and conviction under overbroad statute, "an accused ... does not have to sustain the burden of demonstrating that the State could not constitutionally have written a different and specific statute covering his activities").

n258. Members of the City Council v. Taxpayers for Vincent, 466 U.S. 789, 801 (1984).

n259. U.S. Const. amend. IV.

n260. Tracey Maclin, When the Cure for the Fourth Amendment Is Worse than the Disease, 68 S. Cal. L. Rev. 1, 8 (1994). Indeed, as Maclin notes, "Everyone ... agrees that the Framers opposed general warrants." Id. at 9; see also Leonard W. Levy, Origins of the Bill of Rights 157-58 (1999) (discussing history of colonial opposition to writs of assistance and that history's connection to adoption of Fourth Amendment).

n261. Silas J. Wasserstrom & Louis Michael Seidman, The Fourth Amendment as Constitutional Theory, 77 Geo. L.J. 19, 82 (1988).

n262. See David M. O'Brien, Privacy, Law, and Public Policy 38 (1979); see also Levy, supra note 260, at 150 (describing British use of general warrants and its role in development of Fourth Amendment).

n263. Michael Mello & Paul Perkins, Ted Kaczynski's Diary, 22 Vt. L. Rev. 83, 90 (1997).

n264. It is worth noting that the Fourth Amendment also involves balancing. The government can search nearly anything after meeting the appropriate threshold. But see Winston v. Lee, 470 U.S. 753, 766 (1985) (surgical removal of bullet in suspect's chest, with warrant supported by probable cause, was nonetheless unreasonable under Fourth Amendment). Indeed, the government can even search the intimate sanctuaries of a person's home with a warrant supported by probable cause.

n265. For a detailed discussion of First Amendment balancing, see Daniel J. Solove, The Virtues of Knowing Less: Justifying Privacy Protections Against Disclosure, 53 Duke L.J. 967, 981-89 (2003).

n266. Nadine Strossen suggests importing a "least intrusive alternative" analysis into Fourth Amendment law, which, she argues, would protect a wide range of constitutional rights such as free speech, substantive due process privacy, procedural due process, equal protection, and more. See Strossen, supra note 109, at 1176-77, 1210. The "narrow tailoring" requirement I propose is less stringent than the least intrusive alternative analysis, which is typically employed in cases involving strict scrutiny.

n267. U.S. Const. amend. IV.

n268. Akhil Reed Amar, The Constitution and Criminal Procedure: First Principles 39 (1997).

n269. Christopher Slobogin, The World Without a Fourth Amendment, 39 UCLA L. Rev. 1, 17 (1991).

n270. Probable cause requires that the government have "reasonably trustworthy information" that the search will turn up evidence of a crime. Brinegar v. United States, 338 U.S. 160, 175-76 (1949) (quoting Carroll v. United States, 267 U.S. 132, 162 (1925)).

n271. 44 P.3d 1044 (Colo. 2002).

n272. Id. at 1047.

n273. Id. at 1053.

n274. Id. at 1056.

n275. Id. at 1061-63.

n276. See Zurcher v. Stanford Daily, 436 U.S. 547, 567 (1978) ("We decline to reinterpret the [First] Amendment to impose a general constitutional barrier against warrants to search newspaper premises, to require resort to subpoenas as a general rule, or to demand prior notice and hearing in connection with the issuance of search warrants.").

n277. Eugene Volokh, Deterring Speech: When Is It "McCarthyism"? When Is It Proper?, 93 Cal. L. Rev. 1413, 1448 (2005).

n278. See id.

n279. See Weeks v. United States, 232 U.S. 383, 392 (1914) (arguing that unlawful seizures "should find no sanction in the judgments of the courts"). Morgan Cloud notes that the Fourth Amendment exclusionary rule "is at least implicit in Boyd." Cloud, supra note 140, at 581.

n280. 367 U.S. 643, 655 (1961).

n281. Id. at 655-57 (quoting Bram v. United States, 168 U.S. 532, 543 (1897)). The Court asked rhetorically: "Why should not the same rule apply to what is tantamount to coerced testimony by way of unconstitutional seizure of goods, papers, effects, documents, etc.?" Id. at 656.

n282. Id. at 657.

n283. See supra Part I.D.

n284. See supra text accompanying notes 256-63.

n285. Cf. Berger v. New York, 388 U.S. 41, 56-57 (1967) (discussing how electronic surveillance orders can be crafted so as to be compatible with particularity requirement of Fourth Amendment).

n286. Search engine companies often maintain logs of which IP addresses are connected to particular searches. If provided with a particular IP address, these companies can produce a list of terms searched by that user. IP addresses can be connected to specific individuals by obtaining ISP records about the customer accounts assigned to particular addresses. Hansell, supra note 5; Declan McCullagh & Elinor Mills, Verbatim: Search Firms Surveyed on Privacy, CNET News, Feb. 3, 2006, http://news.com.com/Verbatim+Search+firms+surveyed+on+privacy/2100-1025 3-6034626.html?tag=st.prev.

In 2006, the government attempted to subpoena, inter alia, records of people's Internet search query activity over a two-month period in the summer of 2005. The government sought queries from Yahoo, Google, MSN, and other search companies. Google challenged the request, but the other companies complied. Eventually, the government backed down significantly, asking only for 5000 search queries, but a district court denied even the scaled-down request for search queries as unnecessary. See Gonzales v. Google, Inc., 234 F.R.D. 674, 678, 679, 686 (N.D. Cal. 2006).

n287. See supra Part I.A.

n288. 521 U.S. 844 (1997).

n289. Id. at 853.

n290. Id. at 852.

n291. See supra Part III.A.2.

n292. See supra Part III.B.2.

n293. See 18 U.S.C. §2339A(a)-(b) (Supp. III 2003), amended by USA PATRIOT Improvement and Reauthorization Act of 2005, Pub. L. No. 109-177, 120 Stat. 208 (criminalizing provision of "material support" to terrorists, including "financial services, lodging, training, expert advice or assistance," among other things).

n294. The FBI can obtain an individual's financial records using an NSL if it:

certifies in writing to the financial institution that such records are sought for foreign counterintelligence purposes to protect against international terrorism or clandestine intelligence activities, provided that such an investigation of a United States person is not conducted solely upon the basis of activities protected by the First Amendment to the Constitution of the United States.

12 U.S.C. §3414(a)(5)(A) (Supp. III 2003). The Fair Credit Reporting Act provides for NSLs that allow the FBI to obtain "the names and addressees of all financial institutions... at which a customer maintains or has maintained an account," 15 U.S.C. §1681u(a) (Supp. III 2003), as well as "identifying information respecting a consumer, limited to name, address, former addresses, places of employment, or former places of employment." Id. §1681u(b). According to one estimate, 30,000 NSLs are issued every year. Barton Gellman, The FBI's Secret Scrutiny; In Hunt for Terrorists, Bureau Examines Records of Ordinary Americans, Wash. Post, Nov. 6, 2005, at A1.

n295. 18 U.S.C. §2709 (2000 & Supp. III 2003), amended by USA PATRIOT Improvement and Reauthorization Act of 2005, Pub. L. No. 109-177, 120 Stat. 213.

n296. See supra Part I.B.

n297. 18 U.S.C. §2709(b) (Supp. III 2003); see also 12 U.S.C. §3414(a)(5)(A) (Supp. III 2003) (similar language). The Privacy Act, 5 U.S.C. §552a(e)(7) (2000), also provides some First Amendment protection, requiring that agencies shall "maintain no record describing how any individual exercises rights guaranteed by the First Amendment unless expressly authorized by statute or by the individual about whom the record is maintained or unless pertinent to and within the scope of an authorized law enforcement activity." Id.

n298. 442 U.S. 735 (1979).

n299. Id. at 745-46.

n300. Pen Register Act, 18 U.S.C. §3122 (2000) (requiring court order to obtain pen register information upon showing that such information "is relevant to an ongoing criminal investigation").

n301. USA PATRIOT Act §216, 18 U.S.C. §3123(a) (Supp. III 2003).

n302. But see Patricia L. Bellia, Surveillance Law Through Cyberlaw's Lens, 72 Geo. Wash. L. Rev. 1375, 1403-09 (2004) (arguing that Smith and similar third-party cases should not be extended to communications held by service provider); Deirdre K. Mulligan, Reasonable Expectations in Electronic Communications: A Critical Perspective on the Electronic Communications Privacy Act, 72 Geo. Wash. L. Rev. 1557, 1576-82 (2004) (arguing that there are several limiting principles in business record cases like Smith that prevent their application to e-mail communication).

n303. Cole, supra note 229, at 226.

n304. 18 U.S.C. §3123(a).

n305. Roberts v. U.S. Jaycees, 468 U.S. 609, 618 (1984).

n306. Id. at 622.

n307. 425 U.S. 435 (1976).

n308. Id. at 442-43.

n309. Id. at 444 n.6. For a discussion of how the third-party doctrine cases might be more narrowly interpreted, see the sources cited in note 302, supra.

n310. Miller, 425 U.S. at 444 n.6. (citation omitted).

n311. 416 U.S. 21 (1974).

n312. Bank Secrecy Act of 1970, Pub. L. No. 91-508, §§101-102, 84 Stat. 1114 (current version at 12 U.S.C. §1829(b) (2000)).

n313. See H. Jeff Smith, Managing Privacy 24 (1994) (stating that trend toward reduction in paper records in banking industry made criminal investigations more difficult, leading to adoption of Bank Secrecy Act).

n314. 31 C.F.R. §103.23 (1974); see also id. §103.25 (listing information subject to reporting requirements).

n315. Id. §103.22.

n316. Cal. Bankers, 416 U.S. at 65 (quoting United States v. Morton Salt Co., 338 U.S. 632, 652 (1950)).

n317. Id. at 67-68.

n318. Id. at 71-73.

n319. Id. at 75-76.

n320. Id. at 76 ("Until there is some showing that the reporting requirements contained in the Secretary's regulations would require the reporting of information with respect to the organization's financial activities, no concrete controversy is presented to this Court for adjudication.").

n321. Id. at 78-79 (Powell, J., concurring and joined by Blackmun, J.).

n322. Id. at 78.

n323. Id. at 85 (Douglas, J., dissenting).

n324. Id. at 93 (Brennan, J., dissenting); id. at 97-99 (Marshall, J., dissenting).

n325. United States v. Miller, 425 U.S. 435, 444 n.6 (1976).

n326. 424 U.S. 1 (1976) (per curiam).

n327. Id. at 65-66 (quoting NAACP v. Alabama ex rel. Patterson, 357 U.S. 449, 460 (1958)).

n328. Cole, New McCarthyism, supra note 167, at 11.

n329. See, e.g., Local 1814 v. Waterfront Comm'n, 667 F.2d 267, 272 (2d Cir. 1981) (concluding that subpoena for contributors to Fund violated First Amendment because "compelled disclosure of the Fund's contributors under the circumstances of this case would give rise to a chilling effect similar to the one recognized by the Supreme Court in Shelton v. Tucker"); United States v. Citizens State Bank, 612 F.2d 1091, 1094 (8th Cir. 1980) (finding that antitax group's allegation that subpoena on bank for account records caused "adverse effects" on its "organizational and fundraising activities" was sufficient to establish "a prima facie showing of arguable First Amendment infringement").

n330. 701 F.2d 115 (10th Cir. 1983).

n331. Id. at 118.

n332. Cal. Bankers Ass'n v. Shultz, 416 U.S. 21, 85 (1974) (Douglas, J., dissenting).

n333. One example is when the police use random checkpoints, such as fixed sobriety checkpoints for drivers. Mich. Dep't of State Police v. Sitz, 496 U.S. 444, 455 (1990).

n334. See Illinois v. Lidster, 540 U.S. 419, 427 (2004) ("In judging reasonableness, we look to the gravity of the public concerns served by the seizure, the degree to which the seizure advances the public interest, and the severity of the interference with individual liberty." (internal citations and quotation marks omitted)).

TAB 16

10 of 11 DOCUMENTS

UCLA Law Review

April, 2005

52 UCLA L. Rev. 1149

LENGTH: 38228 words

ARTICLE: Reconciling Data Privacy and the First Amendment

NAME: Neil M. Richards*

BIO: * Associate Professor of Law, Washington University. The author would like to thank the following people who helped immeasurably at the various stages of this project: Sam Bagenstos, Ken Bamberger, Kathie Barnes, Lillian BeVier, Chris Bowers, Trey Childress, John Harrison, Chris Hoofnagle, Peter Joy, Orin Kerr, Pauline Kim, Tom Nachbar, Troy Paredes, Wendy Niece Richards, Bo Rutledge, Joel Seligman, Daniel Solove, Peter Swire, and Eugene Volokh. This Article was also shaped significantly by the participants in law faculty workshops at the University of Virginia, Washington University, the College of William & Mary, the University of Illinois, Ohio State University, and the University of Alabama. Yvonne Ingram and Carol Wibbenmeyer provided invaluable secretarial help, and Sid Karamaju, Matt Kriegel, Megan Dredla, and Matt Bunda provided excellent research assistance.

SUMMARY:
... While these advances permit ever-more efficient and valuable uses of consumer information by businesses, they also raise a cluster of undeniable but poorly defined legal issues about the rights of consumers to participate in, oversee, or control the ways in which data about them is used. ... " Finally, other scholars who might not adopt the strong Volokh-Singleton formulation of the First Amendment critique nevertheless accept its basic premise that data privacy raises real First Amendment issues, and that regulation of consumer privacy needs to be crafted carefully to avoid constitutional objections. ... Looking carefully at whether regulation of information flows and databases is really a regulation of speech within the scope of the First Amendment could thus produce a potentially satisfying doctrinal and theoretical response to the First Amendment critique, allowing us to separate the easy, nonspeech cases away from the minority of cases in which free speech and data privacy are in conflict. ... Moreover, to the extent that law can reinforce social norms, a privacy rule applied to an area where there is no existing social convention of confidentiality could, over time, create new such norms. ... From this perspective, there are some fairly strong parallels between the traditional conception of Lochner and the First Amendment critique of data privacy legislation. ...

HIGHLIGHT: This Article challenges the First Amendment critique of data privacy regulation - the claim that data privacy rules restrict the dissemination of truthful information and thus violate the First Amendment. The critique, which is ascendant in privacy discourse, warps legislative and judicial processes and threatens the constitutionalization of information policy. The First Amendment critique should be rejected for three reasons. First, it mistakenly equates privacy regulation with speech regulation. Building on scholarship examining the boundaries of First Amendment protection, this Article suggests that "speech restrictions" in a wide variety of commercial contexts have never triggered heightened First Amendment scrutiny, refuting the claim that all information flow regulations fall within the First Amendment. Second, the critique inaccurately describes current First Amendment doctrine. To demonstrate this point, this Article divides regulations of information flows into four analytic categories and demonstrates how, in each category, ordinary doctrinal tools can be used to uphold the constitutionality of consumer privacy rules. Third, the critique is normatively unpersuasive. Relying on recent intellectual histories of American constitutional law, this Article

argues that fundamental jurisprudential reasons counsel against acceptance of the First Amendment critique. From the perspective of privacy law, there are striking parallels between the critique's advocacy of "freedom of information" and the discredited "freedom of contract" regime of Lochner. More importantly, from the perspective of First Amendment law, the critique threatens to obliterate the distinction between economic and political rights at the core of post-New Deal constitutionalism. Rejecting the First Amendment critique thus has real advantages. At the level of policy, it preserves the ability of legislatures to develop information policy in a nuanced way. And at the level of theory, it preserves the basic dualism upon which the modern edifice of rights jurisprudence is built.

TEXT:
[*1150]

Introduction

Although private-sector databases containing large amounts of personal information have existed for several decades, a number of recent technological advances and cultural shifts have enabled the easier dissemination of such information and the creation of larger, more detailed, and more useful databases. n1 While these advances permit ever-more efficient and valuable uses of consumer information by businesses, they also raise a cluster of undeniable but poorly defined legal issues about the rights of consumers to participate in, oversee, or control the ways in which data about them is used. Proposals attempting to resolve this so-called "database problem" n2 have been bedeviled by a range of practical and theoretical objections. Foremost among these objections is the widely held belief that because the First Amendment protects **[*1151]** at its core the dissemination of truthful information, any right of "data privacy" is in direct conflict with the First Amendment because any attempt to regulate the flow of personal data would inevitably require the government to impose unconstitutional restrictions on speech. This position, which I call the "First Amendment critique" of data privacy, enjoys widespread currency in the legal academy, the private sector, and recent privacy jurisprudence. For example, Eugene Volokh has argued that "we already have a code of "fair information practices,' and it is the First Amendment, which generally bars the government from controlling the communication of information (either by direct regulation or through the authorization of private lawsuits)." n3

This Article takes issue with the conventional wisdom that regulating databases regulates speech, that the First Amendment is thus in conflict with the right of data privacy, and that the Constitution thereby imposes an insuperable barrier to basic efforts to tackle the database problem. I argue that the relationship between privacy and the First Amendment is complex, but that it is not irreconcilable. Much of the perceived conflict results from an underappreciation of the definitional murkiness that suffuses existing legal conceptions of "privacy" and "speech." Such murkiness has allowed what are essentially consumer protection issues in the economic rights context to be transformed into civil rights issues of the highest magnitude, as opponents of data privacy regulation have seized upon the First Amendment as a handy means of derailing proposals to deal with the database problem. The First Amendment critics overstate the First Amendment issues at stake in the context of most database regulation proposals, because such proposals are not regulation of anything within the "freedom of speech" protected by the First Amendment. Putting First Amendment rights talk to one side allows us to look at data privacy rules more clearly. And this new clarity reveals that a wide variety of these rules are fully justifiable under well-established First Amendment theory, either because they do not regulate "speech" protected by the First Amendment, or because they are legitimate speech regulations under existing doctrine.

My approach has, I believe, significant advantages for both data privacy and free speech. On the privacy side, harmonizing data privacy with free speech removes a significant theoretical and practical obstacle to constructive discussions about, and potential solutions to, the database problem. It also avoids the constitutionalization of domestic information policy, permitting that policy to be developed in a way that reflects the enormous complexity of the issue. And on the speech side, recognizing the murky way that we perceive the **[*1152]** existence of First Amendment problems allows us to assess both speech and nonspeech issues more effectively. More fundamentally, resisting the creep of First Amendment analysis into the economic rights and commercial context preserves the basic and essential division between civil and economic rights at the core of modern constitutionalism.

I develop these claims in four parts. Part I sets forth the data privacy issues raised by the collection, aggregation, and use of large amounts of personal information by private-sector businesses. Next, it sketches the First Amendment critique, which posits that attempts to regulate the database problem through law run directly into the unyielding strictures of the First Amendment. Under this view, data privacy rules that give individuals the right to control how their personal information is used restrict communications between speakers and thus impermissibly burden protected speech. The critique suggests not only that legal protection of data privacy is contrary to current First Amendment jurisprudence, but also that creating new free speech exemptions to permit data privacy "speech restrictions" would have many unfortunate consequences, including providing powerful rationales to support other, less benign speech restrictions. I argue that although the critique raises a host of practical and theoretical problems for data privacy law, information policy, and even free speech theory itself, existing scholarly responses to the First Amendment critique of database regulation are either incomplete or unsatisfying because they grant too much ground to the First Amendment critics with respect to the scope of the First Amendment in this context.

Part II responds to the First Amendment critics by suggesting that the simple logic equating privacy regulation with speech regulation is incorrect. Indeed, this is entirely the wrong way to frame the issue, as it rests on an overbroad conception of the types of rules that are perceived to implicate First Amendment analysis. The First Amendment critics' assumption not only ignores the reality that few data privacy rules actually involve speech, but also significantly overstates the breadth of the protection afforded by the First a protected by the First Amendment, because large categories of "speech" regulations (such as criminal solicitation, anticompetitive offers, and copyright infringement) do not in reality trigger heightened First Amendment scrutiny. Building upon the work of the few scholars to have examined the First Amendment in this way, I suggest that much of this "speech" is either outside the scope of the freedom of speech protected by the First Amendment, or constitutes a hitherto unnoticed category of speech warranting rational basis review. I then defend this conception of the scope of First Amendment analysis against both First Amendment critics and **[*1153]** their pro-privacy opponents, each of whom too readily accepts the presence of a tension or conflict between privacy rules and speech rights.

Following this reconceptualization of the relationship between free speech and privacy, Part III responds to the First Amendment critique in more detail, demonstrating how existing doctrine fully supports a wide variety of privacy regulations without violating the First Amendment. In order to assess and demonstrate the constitutionality of such rules more easily, I divide privacy rules that implicate information flows into four categories: collection rules, use rules, disclosure rules, and telemarketing rules. Information collection rules, which govern the circumstances under which persons can collect information about others, create virtually no First Amendment problems and have been upheld in a wide variety of contexts. Similarly, information use rules also raise few issues of constitutional magnitude, because our law does not consider the use of information to make decisions to be "speech" any more than collecting information is "speaking." While information disclosures are a harder case than use or collection, I demonstrate that, when properly conceptualized, nondisclosure rules in the database context do not significantly implicate the First Amendment. Regulating how two parties to a commercial transaction act with respect to information received during that transaction no more offends the Constitution than does government regulation of other aspects of the commercial relationship. Indeed, our law is replete with instances in which confidential information is protected against disclosure under a whole host of public and private law rules, few of which have ever been thought to involve restrictions on speech. Finally, I address direct regulation of telemarketing, and argue that although such regulation certainly implicates the commercial speech rights of telemarketers, the First Amendment nevertheless permits significant regulation of telemarketing activity. Accordingly, I argue, ordinary data privacy rules are fully consistent with the First Amendment.

Finally, Part IV contends with the First Amendment critique at a more abstract level, placing the critique in its historical and jurisprudential context. I argue that when viewed from the twin perspectives of privacy law and First Amendment law, the real theoretical problems of the First Amendment critique are made manifest. From the privacy law perspective, the modern First Amendment critique of data privacy regulation will, if it is unchallenged, prohibit discussion and resolution of the tremendously thorny database problem, thereby constitutionalizing national information policy and placing its resolution outside the democratic process. Indeed, the parallels are striking between the strong

form of the First Amendment critique and the discredited "liberty of contract" doctrine of the Lochner period. Drawing upon **[*1154]** recent scholarship treating legal history as a species of intellectual history, I argue that both Lochner and the First Amendment critique represent responses to the leading economic public policy issue of their day with a liberal theory of rights constitutionalism that is fundamentally flawed. Finally, looking at the critique from the First Amendment law perspective, I argue that the broad, expansive, and slippery conceptualization of the First Amendment at the core of the First Amendment critique is ultimately inconsistent with the basic dualist premise of modern constitutionalism - the bifurcated standards of judicial review given to civil versus economic rights. I assert the critique paves the way for the obliteration of the distinction between economic and civil rights at the core of post-Lochner American constitutionalism. Serious recognition of the First Amendment critique would result not only in the constitutionalization of a major and complex policy issue, but also would threaten to unravel the basic premise upon which post-New Deal constitutionalism is based.

I. The First Amendment Critique of Data Privacy Regulation

Scholars exploring the conflict between the right of privacy and the First Amendment have traditionally located its origins with the publication of Samuel Warren and Louis Brandeis's foundational 1890 article "The Right to Privacy." n4 In their article, Warren and Brandeis sought to establish a common law tort of "privacy" to protect principally against intrusions by an overzealous media. n5 Although a conflict between privacy and speech might thus seem inevitable, this conclusion is belied somewhat by the fact that both privacy law and modern First Amendment doctrine can trace their origins back to the turn of the twentieth century when both were guided significantly by the writings of Louis Brandeis. Thus, while Brandeis's famous Harvard Law Review article is widely understood as the progenitor of twentieth-century privacy law, n6 his concurrence in Whitney v. California n7 has been equally influential in the creation and development of modern free speech jurisprudence. n8

[*1155] Although privacy and speech have shared an uneasy coexistence in American law, this tension is a product of a conceptual murkiness shared by both doctrines, rather than any fundamental incompatibility. Despite its recognition for over a century, n9 the right to privacy has been poorly articulated and only vaguely theorized. As a result, modern commentators despair at ever being able to define "privacy" coherently. n10 Although the First Amendment has received greater theoretical attention by judges and scholars, latent murkiness in First Amendment theory also persists, exacerbating the perceived tensions with privacy theory. n11 Nevertheless, when the First Amendment and privacy have come into conflict in the past, most significantly in a long line of Supreme Court cases invalidating attempts to impose liability on the press for committing the tort of disclosure of private information, the First Amendment has universally triumphed. n12 Such a result is undoubtedly consistent with the basic tenet of modern constitutional law that public discussions of issues of matters of public concern "should be uninhibited, robust, and wide-open." n13 Modern First Amendment critics of data privacy regulation hearken back to this long tradition of privacy being in tension with the First Amendment, with privacy inevitably losing out when weighed against the constitutional primacy of free speech. And although defenders of privacy have struggled to articulate a theory whereby privacy rules can withstand First Amendment scrutiny, few scholars have been able to articulate persuasive justifications why any right of data privacy should survive when pitted against the robust modern First Amendment. n14

With this context in mind, I attempt in this part to frame the basic problem facing scholars, judges, and lawmakers confronting the conceptual intersection of data privacy and the First Amendment. First, I briefly describe the database problem in order to identify the practical stakes in this often theoretical debate. Second, I describe the First Amendment critique of data privacy regulation. I argue that no compelling response to the First Amendment critique has yet been fully articulated in the privacy literature; although a few scholars have attempted to take on the First Amendment critics, their arguments are neither complete nor convincing.

[*1156]

A. The Database Problem

There is a vast and often redundant literature describing the database problem, and I have no intention of adding to it here. n15 However, a brief overview of the contours of the problem will be helpful in setting up and contextualizing the analysis that follows. Governments have been keeping records about their citizens for centuries, most notably tax and criminal records. n16 In the nineteenth century, the federal census raised what we would today call privacy concerns and federal law was amended to protect the confidentiality of information collected by the government. n17 In the twentieth century, with the expansion of American government during and after the New Deal period, dozens of national government agencies including the FBI, the Internal Revenue Service, the military, and the Social Security Administration began keeping trillions of records on individual citizens. n18 The invention and spread of increasingly cheaper and more capable computers only facilitated this process, particularly as the use of social security numbers as uniquely effective personal identifiers enabled agencies to link records and integrate them with other databases, including state and private databases. n19 As the Supreme Court has recognized, modern government possesses an "accumulation of vast amounts of personal information in computerized data banks or other massive government files," including information taken from "the collection of taxes, the distribution of welfare and social security benefits, the supervision of public health, the direction of our Armed Forces, and the enforcement of our criminal laws." n20

Public sector databases do create significant privacy problems, including increasing the risk of identity theft, chilling expressive but eccentric behaviors, revealing embarrassing information to private parties, and raising the specter of an Orwellian state. n21 But such problems can be addressed (at least **[*1157]** at a theoretical level) through ordinary public law rules without any significant constitutional impediments. n22 No one suggests that the government has a right to publish any and all secrets it learns about its citizens absent a need to do so; indeed, the Supreme Court has stated on several occasions that individuals have a constitutional right to prevent the government from making public at least certain kinds of information about themselves. n23

The same technological advances that have permitted the creation of public sector databases have also allowed businesses and other private-sector entities to keep ever larger and more detailed records about individuals. These records can be created from a variety of sources, including publicly available government records, human resource databases, promotional activities such as contests and mass mailings, and transactional data from noncash purchases, frequent shopper programs, and Internet and telephone use. n24 Information collected from these sources often has more value as a saleable commodity than for the purposes for which it was originally collected. Indeed, corporations are eager to acquire many different kinds of information about consumers, including information about their lifestyles, tastes, and even psychological profiles. n25 Such information is provided by the "profiling industry," a group of companies that aggregate information contained in private databases to create consumer profiles that are then offered for sale to interested parties, be they private or public. n26 The level of detail contained in such profiles is striking, and can include information such as a person's social security number, shopping preferences, health information (including diseases and disorders suffered), financial information, race, weight, clothing size, arrest record, lifestyle preferences, hobbies, religion, reading preferences, homeownership, charitable contributions, mail order purchases and type, and pet ownership. n27 Such information can be bought for as little as $ 65 per thousand **[*1158]** names, categorized by the type of consumer sought by marketers. n28 One profiling company was reported to have personal and private information about virtually every consumer in the United States, Britain, and Australia. n29 In addition to being intrusive and deeply unsettling to many people, the multibillion dollar profiling industry provides the lifeblood of data on which the direct marketing industry survives. n30

At the practical level, such activities raise at least four kinds of privacy concerns. First, databases can be used to process "sensitive information" - nonnewsworthy but nonetheless potentially embarrassing or highly personal information. Most people would be horrified if this information floated freely from database to database. Second, "uber-databases" can be created, composed of nonsensitive information in such enormous quantities that the database constitutes a highly detailed dossier of a person's entire existence. n31 Third, the information contained in consumer profiles can be quite inaccurate. n32 Finally, there are no meaningful legal requirements that personal information in consumer profiles be kept securely. If used improperly, the sheer level of detail contained in consumer profiles can facilitate crimes such as identity theft, n33 stalking, n34 or harassment. n35

Large-scale private databases also significantly raise the stakes for government surveillance. Governments have long used private records to spy upon their citizens - often with sinister consequences n36 - and the availability of **[*1159]** larger and more detailed private records about people makes such forms of surveillance easier for governments to engage in. n37 Indeed, recent activities by the federal government to investigate and forestall terrorism have frequently relied on computerized private-sector customer records containing financial, airline passenger, and other data. n38 The government also has been contracting increasingly with private businesses, by acquiring databases of personal information and funding novel private-sector data collection projects. n39 To the extent such private data collection is not state action, it allows the government, in effect, to outsource surveillance beyond the scope of otherwise applicable statutory and constitutional restrictions. n40

Database privacy is a complex problem, and database regulation would be costly. n41 This is particularly true insofar as privacy regulations by their very nature would tend to keep information away from individuals who would like to see it, be they employers, credit card companies, potential spouses, or even journalists. And regulation of profiling practices would provide, at a minimum, significant economic costs to that industry. But many scholars have argued that there are other costs to privacy regulation. Kent Walker asserts that "legislating privacy comes at a cost: more notices and forms, higher prices, fewer free services, less convenience, and, often, less security." n42 Some commentators have argued that broad privacy rules would not only be costly, but also could lead to unintended consequences such as a decrease in self-regulation, services offered to the public, and data made available for research. n43 Law and economics scholars like Richard Posner conclude that privacy rules inefficiently decrease the total supply of information, increase **[*1160]** transaction costs, and encourage fraud. n44 Others extend this argument and claim that the inefficiency of privacy rules means that consumers are actually better off with less privacy regulation than with more, as the free, unfettered flow of information leads to a socially optimal result of lower prices for consumers. n45

B. The First Amendment Critique

The foregoing has not intended to propose regulatory solutions to the database problem, but merely to suggest that this problem is important, complex, and demands serious and thoughtful deliberation before it can be resolved in any meaningful way. Indeed, the database problem has produced no shortage of proposals seeking to address its privacy implications. n46 But virtually all such proposals run squarely into what I call the "First Amendment critique": the claim that because the creation, assembly, and communication of information are at the core of the First Amendment, data privacy rules that restrict this expressive activity improperly burden free speech and are thus largely or entirely unconstitutional. The First Amendment critique is a significant theoretical and practical obstacle to data privacy regulation because it asserts that the First Amendment automatically resolves any privacy policy issues created by the database problem by preventing any regulatory solution that impinges upon the free flow of information. The simplicity and salience of the critique have caused it to become part of the conventional wisdom in the data privacy debate. n47 Indeed, privacy scholars have **[*1161]** been unable to refute the critique, n48 allowing it to dominate both constitutional jurisprudence and democratic policymaking with respect to data privacy.

The most prominent First Amendment critic is Eugene Volokh. Volokh starts from the proposition that although data privacy sounds unthreatening in the abstract, "the difficulty is that the right to information privacy - my right to control your communication of personally identifiable information about me - is a right to have the government stop you from speaking about me." n49 Accordingly, while private agreements to restrict speech are enforceable under express and implied contract principles, any broader, government-imposed code of fair information practices that restricts the ability of speakers to communicate truthful data about other people is inconsistent with the most basic principles of the First Amendment. n50 Indeed, Volokh goes so far as to conclude that "despite their intuitive appeal, restrictions on speech that reveals personal information are constitutional under current doctrine only if they are imposed by contract, express or implied." n51 Volokh's argument can be boiled down to two basic elements: First, data privacy regulation that restricts the communication of information and that is not grounded in contract violates the First Amendment; and second, the changes to existing doctrine necessary to permit data privacy rules could be used to justify other, more sinister exceptions to free speech doctrine. n52

Other scholars make arguments similar to Volokh's. Relying on the Supreme Court cases invalidating the privacy tort in the context of media publication of truthful facts, Fred Cate has argued more bluntly that electronic information flows should be entitled to full First Amendment protection, and that any attempt to restrict the communication of truthful data faces a high (if not insurmountable) First Amendment obstacle. n53 Solveig Singleton also suggests that efforts to regulate consumer privacy in the database **[*1162]** context run squarely into established First Amendment limits on government power. n54 Singleton concludes "there is no justification for regulating the collection and use of data by the private sector. Regulations intended to protect privacy by outlawing or restricting the transfer of consumer information would violate rights of free speech." n55 The critique has resonated not just with numerous scholars of a conservative or pro-business bent, n56 but also with liberal First Amendment scholars such as Robert O'Neil, n57 Rodney Smolla, n58 and Michael Froomkin. n59 Laurence Tribe has also argued publicly that the processing of personal data by telephone companies is speech entitled to full First Amendment protection. Tribe argued that such data is created and assembled by telephone companies for marketing, and that "the First Amendment protects [a speaker's] right not only to advocate their cause but also to select what they believe to be the most effective means of so doing." n60 Finally, other scholars who might not adopt the strong Volokh-Singleton formulation of the First Amendment critique nevertheless accept its basic premise that data privacy raises real **[*1163]** First Amendment issues, and that regulation of consumer privacy needs to be crafted carefully to avoid constitutional objections. n61

The salience of the First Amendment critique in academic and legal discourse has influenced both courts and policymaking. As a result, the First Amendment critique is a major obstacle to coherent data privacy regulation. Two recent cases illustrate the jurisprudential uncertainty that the critique has fomented. In U.S. West, Inc. v. FCC, n62 the Tenth Circuit struck down as an unconstitutional burden on commercial speech a rule imposing a duty of confidentiality upon telephone companies with respect to customer data collected in the course of providing telephone service. Similarly, the First Amendment critique played a significant role in the recent litigation over the FCC's "Do-Not-Call" Registry, which allows consumers who do not wish to receive commercial telemarketing calls to place their telephone numbers on a list of numbers that telemarketers are forbidden from calling. n63 Applying the critique, a federal district court invalidated the Registry as an unconstitutional infringement on commercial speech. n64 Although the Tenth Circuit correctly n65 **[*1164]** reversed the lower court on appeal, n66 the First Amendment critique nevertheless seriously complicated resolution of the issue, with the constitutionality of the Registry in limbo for months. Despite the ultimately satisfactory resolution of the Do-Not-Call litigation from a privacy perspective, courts remain deeply divided over the salience of the critique. n67 The Supreme Court has said little with respect to this issue, and has not granted certiorari to clear up the confusion among lower courts. n68

In addition to its effects on litigation, the First Amendment critique is a potent weapon against privacy rules in the legislative process. Perhaps because the critique is an easy political argument for opponents of regulation to make, and because it invites litigation whenever new privacy measures are enacted, lawmakers and regulators are likely to take the critique into account in drafting privacy rules, thereby skewing the outcome of such deliberative processes. For example, when the State of Washington attempted to pass a privacy bill in early 2000, the attempt was scuttled by business groups proffering Professor Volokh's claims that the free flow of commercial information is constitutionally compelled. n69 These examples illustrate the practical significance of the First Amendment critique - the confusion and discord that it is causing in both democratic policymaking and the courts.

Perhaps because of the inherent appeal of First Amendment arguments generally to legal academics (especially those who tend to support privacy rights), n70 surprisingly few scholars have challenged the First Amendment critique in any detail. Indeed, although a handful of scholars have disagreed with the arguments of Volokh and others who advocate the critique, they **[*1165]** have done so either in short essays or in sections of longer pieces. n71 This is unfortunate, because the First Amendment critique asserts a simple, constitutionalized solution to a complex and thorny social problem of the first importance. To be clear, I believe that the simplistic mantra of "freedom of information" is no more a satisfying solution to the complex database problem facing the digital age than the "freedom of contract" was to the industrial age a century ago. n72 In the rest of this Article, I lay out a series of doctrinal, conceptual, and jurisprudential responses to the First Amendment critique. Reconceptualizing the First Amendment issues at stake in the

database context reveals that the policy choices behind the regulation of private information in the computer age are not foreordained by the First Amendment.

II. Are Privacy Rules Speech Rules?

One of the basic assumptions of the First Amendment critics is that regulating privacy is the same as regulating speech. This view is best summarized by Eugene Volokh, who argues:

> The right to information privacy - my right to control your communication of personally identifiable information about me - is a right to have the government stop you from speaking about me. We already have a code of "fair information practices," and it is the First Amendment, which generally bars the government from controlling the communication of information (either by direct regulation or through the authorization of private lawsuits), whether the communication is "fair" or not. While privacy protection secured by contract is constitutionally sound, broader information privacy rules are not easily defensible under existing free speech law. n73

This part tackles and rebuts this foundational assumption at the conceptual level. Although there exists much ambiguity not only in privacy law but also in the **[*1166]** scope of the First Amendment, there are definite, significant areas in which the two do not conflict. I hope to show that substantial regulation of privacy rights is possible without implicating the First Amendment at all, thereby setting the stage for a doctrinal and jurisprudential reconciliation in subsequent parts between the First Amendment and the right of data privacy.

Part II.A addresses the fundamental assumption of the First Amendment critics that privacy regulation means speech regulation. I argue that most data privacy regulations in the form of a "code of fair information practices" have nothing to do with free speech under anyone's definition. Part II.B focuses on the regulation of information flows and suggests that the First Amendment accords heightened scrutiny to far fewer regulations of "speech" than previous scholars have assumed. I argue that First Amendment critics and the few privacy scholars to have responded to them have improperly conflated information flows - such as the sale of a database - with the "freedom of speech" protected by the First Amendment. In my view, there are valid First Amendment reasons for drawing distinctions between speech and information flows. Recognizing such distinctions provides a superior way of conceptualizing the First Amendment implications of the database problem.

A. Privacy Regulation Through Codes of Fair Information Practices

Regulation of the collection, use, and disclosure of personal data is often proposed as a code of fair information practices. n74 Such proposals call for a combination of tort and public law to regulate the relationship between the individuals who provide data and the entities that would collect, use, and disclose it. n75 One early code of fair information practices was envisioned by the federal Department of Housing, Education, and Welfare in 1973, which recommended that organizations collecting data should adhere to a series of norms. These included a prohibition on secret data collection, a right of access by individuals to view data about themselves and correct false data, and a right to prevent information collected for one purpose from being used for other purposes. n76 This report was the basis for the federal Privacy Act of 1974, n77 which established general rules for the collection, retention, use, and disclosure **[*1167]** of personal information held by the federal government. n78 In particular, Section (e) of the Privacy Act mandates that federal agencies follow fair information practices. n79

The norms established by the Housing Department's report and the Privacy Act have been tremendously influential in the United States and other countries, and many scholars agree that there is a global consensus regarding the basic standards of fair information practices for both the public and private sectors. n80 Joel Reidenberg has summarized this consensus as guaranteeing four protections against data misuse: (1) standards for data quality, which ensure that data is acquired legitimately and is used in a manner consistent with the purpose for which it was acquired; (2) standards for

transparency or openness of processing, such as giving individuals meaningful notice regarding how their information is being used; (3) special protections for sensitive data (for example, race, sexual preference, political views, or telephone numbers dialed), such as requiring opt-in consent before such data may be used or disclosed; and (4) some standards of enforcement to ensure compliance. n81

Recognizing the similarity between the privacy issues in the public and private-sectors, numerous state and federal laws impose codes of fair information practices in a variety of private-sector contexts. Such statutes attempt to protect consumers from inappropriate uses of personal data by businesses. n82 Federal examples of such laws include the Fair Credit Reporting Act, n83 the Electronic Communications Privacy Act (ECPA), n84 the Video Privacy Protection Act (VPPA), n85 and the Family Educational Rights and Privacy **[*1168]** Act. n86 Violations of such federal codes of fair information practices for the private sector are punished by both criminal law prosecutions and private tort law actions, which authorize significant minimum statutory and punitive damages. n87

Statutes that embody fair information principles do far more than merely regulate information flows or prevent disclosures. Paul Schwartz has argued that under Reidenberg's four-part taxonomy of fair information practices, principle one (ensuring data quality), principle two (ensuring transparency of processing), and principle four (ensuring enforcement) simply have nothing to do with speech under anyone's definition. n88 Only principle three (providing protection against the use or disclosure of sensitive data) "corresponds to Volokh's idea of information privacy as the right to stop people from speaking about you." n89 Although I agree that many fair information practices do not regulate speech, if the First Amendment critics are correct that principle three nondisclosure rules are speech restrictions that violate the First Amendment, it follows that government enforcement of such rules under principle four by either direct regulation or the enforcement of tort judgments similarly violates the First Amendment. But, as I demonstrate below, nondisclosure rules, just like other elements of fair information practices applied to commercial databases, are fully consistent with the First Amendment. The most important point to take from the preceding discussion, however, is that even if one accepts that nondisclosure rules create First Amendment problems, significant forms of information privacy protection envisioned by codes of fair information practices and protected by current laws have nothing whatsoever to do with the First Amendment under anyone's reading.

B. The Constitutional Metaphysics of "Speech"

The insight that information privacy rules are usually modeled upon a code of fair information practices allows us to separate out many of the types of privacy regulations that have nothing to do with speech. It also shows that the rhetorical suggestion that all privacy rules are speech rules is significantly **[*1169]** overblown. But Schwartz and Reidenberg's typology merely tells us that while some parts of a code of fair information practices regulate information flows, much of a typical code has nothing to do with information flows. Their model does not ultimately help us with the really hard question at the core of the First Amendment critique - the constitutional status of information flow regulation. n90

The critics argue that regulation of information flows is regulation of speech, and that free information flows are therefore as constitutionally mandated as free speech. What then do we make of this claim that information flow regulation is a "right to stop other people from speaking about you"? n91 I believe that most privacy regulation that interrupts information flows in the context of an express or implied commercial relationship is neither "speech" within the current meaning of the First Amendment, n92 nor should it be viewed as such. n93 By contrast, the handful of scholars who have previously responded to this question have tended to assume that all information flows are speech, and then disagreed about whether the First Amendment allows or prohibits various forms of privacy regulations. In so doing, these scholars have rejected the notion that at least some forms of data flows might fall outside the scope of heightened First Amendment protection. n94 But by neglecting to consider the boundaries of the First Amendment, scholars seeking to reconcile privacy regulation with the First Amendment have conceptualized the problem improperly, and thereby have missed an important opportunity to explain precisely why privacy rules are fully consonant with our traditions of robust protection for free speech.

Is it conceptually possible to treat commercial information flows as falling outside the "freedom of speech" that the First Amendment protects? That is, even if the critics are correct that the creation or sale of a database is a "communication" of information, is that communication necessarily speech that warrants heightened scrutiny under the First Amendment? Making this determination requires an assessment of the boundaries of First Amendment protection. Unfortunately, in spite of the importance of the First Amendment **[*1170]** to American legal and political culture, n95 very little has been written on the line between the "freedom of speech" protected by the First Amendment and that which is not protected. This lack of attention is even more surprising when one considers the large number of First Amendment cases decided by the Supreme Court alone over the past four decades, n96 as well as the even more voluminous bulk of First Amendment scholarship by legal and other academics. n97

The handful of scholars who have studied this issue suggest that a freedom of speech n98 challenge to a regulation requires a court to answer two questions. The first question is whether there is a First Amendment issue in the first place - whether the regulation infringes upon the "freedom of speech" that the First Amendment protects. The scholarship addressing this issue frames the question as one involving the "coverage," n99 the "boundaries," n100 the "ambit," n101 or most commonly the "scope" n102 of the First Amendment. This question - what I will call the "scope question" - asks whether the activity in question is speech that the First Amendment protects at all.

If the answer to the scope question is "yes," the Court must answer a second question. This question focuses on the "level" n103 of "obligation" n104 or strength of First Amendment "protection." n105 In answering the second question, a court must determine what portion of "the full arsenal of First Amendment rules, principles, standards, distinctions, presumptions, tools, factors, and three-part tests becomes available to determine whether the particular speech will actually wind up being protected." n106 I call this question the "level of protection" question.

[*1171] Courts and scholars invariably focus upon the level of protection question in First Amendment analysis, with the unfortunate result that the scope question has been significantly understudied. Nevertheless, the scope question remains a critical one. The initial work done in this area by Kent Greenawalt on language, speech, and crime concluded that even though much of what the criminal law punishes is "speech" within the common dictionary or lay understanding of the term, imposing criminal punishment for speech is rarely, if ever, considered to raise First Amendment concerns. n107 Thus, we do not perceive the speech used to engage in fraud, to make criminal threats, to form and advance conspiracies, or to solicit criminal acts as First Amendment speech. n108 Punishment imposed on such speech is, both doctrinally and theoretically, not an "abridgement" of the "freedom of speech." n109 Frederick Schauer has expanded Greenawalt's list beyond the criminal context, noting that the First Amendment does not apply to government regulations of speech in the contexts of securities, antitrust, labor organizing, copyrights, trademarks, sexual harassment, the regulation of doctors, lawyers, and other professionals, and vast amounts of evidence and tort law. n110 Schauer argues that the fact that the First Amendment's boundaries are much narrower than the ordinary understanding of the word "speech" suggests the need for further study of the concept of "constitutional salience" - "the often mysterious political, social, cultural, historical, psychological, rhetorical, and economic forces that influence which policy decisions surface as constitutional issues and which do not." n111

Unfortunately, calling things "speech" or "not speech" and thereby placing large areas of speech beyond the scope of the First Amendment tends to make people nervous. There is, however, an alternative method of approaching the inquiry. Rather than looking at which communications are "speech" and which are "not speech," it is possible to view the category of "unprotected" speech as something like the rational basis category that exists in other areas of rights jurisprudence, but which never has been articulated in the context of the First Amendment. Under this approach, all "speech" would be covered by the First Amendment, but the scope question could be viewed as a threshold for invoking heightened scrutiny in much the same way that **[*1172]** suspect classification analysis performs this role in equal protection and due process jurisprudence. "Speech," in the ordinary sense of the term, that fails the scope question would receive rational basis review. For example, in Equal Protection Clause jurisprudence, a court assessing the constitutionality of a classification must compare the type of classification with the list of so-called "suspect classes." While racial classifications receive strict scrutiny and classifications made on the basis of sex receive intermediate scrutiny, classifications involving economic rights receive minimal judicial scrutiny. n112 Similarly, in the due process

context, economic rights are assessed under rational basis review, while the existence of a "fundamental right," such as reproductive autonomy or the right to vote, increases the level of scrutiny. n113

Viewed in this way, the scope and level of protection questions in First Amendment analysis would operate in a similar manner: The scope question determines whether heightened scrutiny is warranted, and if it is, the level of protection question allocates the appropriate doctrinal formulation with which to assess the constitutionality of the speech restriction. For example, regulation of the content of political speech broadcast from a loudspeaker van would be assessed under a strict scrutiny standard, while a content-neutral regulation of the noise level emanating from such a van would be assessed under intermediate scrutiny. n114 But economic regulation of the market for loudspeakers or electrical appliances would receive rational basis review.

Critically, then, just as a classification falling outside one of the suspect categories in equal protection analysis would receive rational basis review, so too would regulations of speech falling outside the scope of the First Amendment. Speech in this category, whether we call it "unprotected speech" or "speech outside the scope of the First Amendment," is merely speech within the dictionary definition of the term that does not warrant heightened protection against government regulation. This might be the case because the speech is threatening, n115 obscene, n116 or libelous, n117 and thus part of the "established" categories of "unprotected speech." But it might also be the case because **[*1173]** the speech is an insider trading tip, n118 a false statement in a proxy statement, n119 an offer to create a monopoly in restraint of trade, n120 or a breach of the attorney-client privilege. n121 In either case, the speech would be outside the scope of the First Amendment and could be regulated as long as a rational basis exists for so doing. Such an approach to First Amendment analysis is not just descriptively accurate, but is entirely defensible under current doctrine, because the freedom of speech is one of the "fundamental rights" protected by the Fourteenth Amendment's Due Process Clause against the states. n122

In the specific context of privacy and speech, this approach would work in an identical fashion. Ordinary public and private law rules regulating businesses engaged in the trade in customer data would be, like other forms of commercial regulation, outside the scope of the First Amendment and thus subject to rational basis review. n123 Examples of such laws would include a paradigmatic code of fair information practices regulating the commercial assembly, processing, and use of large-scale consumer databases. Such regulations would constitute "laws of general applicability" under current doctrine and would not warrant heightened judicial scrutiny beyond the deferential standard applied to most economic regulations. By contrast, regulations of privacy rules that restrict protected speech or that burden conduct with a significant expressive component would fall within the scope of the First Amendment. Such regulations would thus warrant heightened judicial scrutiny. For example, regulation of speech on matters of public or general concern (such as articles in Consumer Reports, disclosure of newsworthy private facts about individuals, discussions of the merits of particular companies, or even some gossip about individuals) would warrant heightened (and most likely strict) scrutiny. Other forms of lesser-protected speech such as telemarketing n124 or regulation of conduct **[*1174]** with a significant expressive component (such as a law outlawing cameras) n125 would receive intermediate scrutiny under the commercial speech doctrine. But the ordinary regulation of the commercial data trade would receive only rational basis review, just as the economic regulation in our loudspeaker example would.

To be clear, I believe that this model accurately describes the way First Amendment law implicitly approaches the scope question. I also believe, however, that this approach is normatively superior to the current conceptual framework used by scholars, who too often neglect the scope question. Looking at restrictions of "speech" in terms of the scope question first can provide a way of resolving their First Amendment status without forcing them into existing doctrinal categories into which they might not fit well. Looking carefully at whether regulation of information flows and databases is really a regulation of speech within the scope of the First Amendment could thus produce a potentially satisfying doctrinal and theoretical response to the First Amendment critique, allowing us to separate the easy, nonspeech cases away from the minority of cases in which free speech and data privacy are in conflict. Such an approach has at least two additional advantages. First, by separating the regulations that threaten First Amendment values from those that do not, it is possible to have a more honest debate about the public policy implications of additional privacy protections in the database context. The benefits and pitfalls of privacy rules can thus be debated on

their own merits by scholars and by legislative bodies, free from the unnecessary, distracting, and discourse-distorting effects of fundamentally spurious First Amendment arguments. Such a discussion is, as I have suggested, currently being short-circuited by constitutional objections when privacy rules are drafted and by needless First Amendment litigation after their enactment. n126 And when such litigation does arise, this approach avoids having the merits of the regulations at issue settled after judicial proceedings in which policy arguments are forced to masquerade as theories of constitutional interpretation. Second, by separating out the easy cases, we can more easily focus on providing doctrinal and theoretical solutions to the really difficult (and important) ones - cases in which the First Amendment and privacy are actually in conflict.

The First Amendment critics would, I imagine, have two responses to this approach. First, they would argue that the exceptions to the scope of the First Amendment are few, defined, and narrowly construed, covering only such established doctrinal categories as obscenity, "incitement, false **[*1175]** statements of fact, threats, and the like." n127 Second, they would argue that even though new exceptions could certainly be created, doing so would create a pernicious and dangerous precedent for other, more nefarious exceptions to protected free speech in the future. n128

With respect to the first argument, I am not convinced that the critics accurately describe the universe of free speech cases. The First Amendment critics are correct that the Supreme Court has held that much of what we think of as communicative speech falls within the scope of the First Amendment, and the Court has also held a few categories to be outside the scope and thus to constitute "unprotected speech." But the Court has never held in a blanket fashion that all communications fall within the scope of the First Amendment and are thus subject to heightened protection. Indeed, as the examples identified by Greenawalt and Schauer reveal, there are many areas of law regulating the content of speech that are not thought to be within the scope of the First Amendment as either a doctrinal or theoretical matter. n129 And as Schauer has argued in responding to an analogous claim, to take the position of the First Amendment critics

is to be afflicted with the common ailment of spending too much time with the casebooks - defining the domain of constitutional permissibility by reference to those matters that have been considered viable enough to be litigated in, and close enough to be seriously addressed by, the courts, especially the Supreme Court. But if we are interested in the speech that the First Amendment does not touch, we need to leave our casebooks and the Supreme Court's docket behind; we must consider not only the speech that the First Amendment noticeably ignores, but also the speech that it ignores more quietly. n130

As a descriptive matter, then, the universe of speech within the scope of the First Amendment, as defined by existing case law, is significantly smaller than the universe of "speech," as understood by the dictionary or lay definition, because the universe of "exceptions" to the Free Speech Clause is far greater than is conventionally thought. n131

[*1176] If the First Amendment critics are thus wrong as a descriptive or interpretive matter about the universe of speech, what about their second claim that creating "new" exceptions to existing doctrinal categories would be a bad idea? Eugene Volokh argues that the changes in jurisprudence necessary to reconcile data privacy with the First Amendment - whether by creating new data privacy exceptions to existing free speech doctrine, or expanding existing exceptions such as commercial speech doctrine - would open the door for a variety of other, more sinister speech restrictions. For example, Volokh argues that widening the exception for speech on matters of private concern would give a strong argument to those who wish to restrict other types of "private" speech that do not address matters of public concern, such as sexually themed speech ranging from "pornography to art to sexual humor." n132 Similarly, he suggests, broadening commercial speech doctrine to accommodate data privacy speech restrictions would stretch the doctrinal category to such a degree that many types of socially beneficial speech and commentary about economic matters would also fall into the category of regulatable commercial speech, "giving the government an ill-defined but potentially very broad power to restrict such speech." n133

I am not convinced by Volokh's slippery slope argument, for three reasons. First, treating the sale of a consumer

database as outside the First Amendment does not create a "new exception" to existing doctrine. To the contrary, there is very little authority assessing the constitutional status of rules of this sort, which suggests that these regulations have never been thought to raise First Amendment problems. n134 Rather than creating a "new exception" to existing doctrine, such restrictions more likely fall as a descriptive matter into what Schauer terms the "speech that [the First Amendment] ignores more quietly." n135

[*1177] Second, Volokh's argument takes issue with the very process by which the Supreme Court has structured First Amendment review since at least New York Times Co. v. Sullivan, n136 in which it sketched the modern formulation for how state tort rules that implicate First Amendment concerns should be evaluated. Rather than engaging in the often treacherous task of balancing the values and harms of speech in particular cases, the Supreme Court in Sullivan articulated the theory of what scholars have called "definitional" n137 or "categorical" n138 balancing. Under this approach, the Court balances the interests involved in a class of speech and sets the level of scrutiny for all cases that fall within the class. In the context of privacy rights, just as in the context of the intersection between tort law and free speech generally, the Supreme Court has settled on a categorical balancing approach to resolve the conflict between privacy claims and free speech. n139 Volokh may disagree with this approach, but to the extent he argues that creating privacy exemptions under the First Amendment violates the First Amendment, his slippery slope argument appears either to criticize a significant portion of the same free speech jurisprudence he seeks to protect, or implicitly to propose a radical departure from that jurisprudence.

Third, Volokh's argument rests on the premise that creating new "exceptions" from the protection of the First Amendment creates "doctrinal, political, and psychological" arguments for creating other exceptions to the First Amendment by analogy, and that the creation of such exceptions is likely to occur in practice. n140 Although he claims that he is not making a slippery slope argument of a "today this speech restriction; tomorrow the Inquisition" sort, n141 his argument is confessedly some form of slippery slope argument, even if it is a more nuanced one than most. In that regard, Volokh's theoretical claim is undercut significantly by the way that the Supreme **[*1178]** Court has actually decided free speech cases over the past half-century. Although the Supreme Court has established several categories of speech that do not enjoy either full protection as core speech n142 or any protection whatsoever, n143 these categories have tended to shrink over time, rather than to grow. For example, although the Supreme Court in the 1940s generally supported free speech rights, n144 it did carve out at least two categories of speech as unprotected by the First Amendment - "fighting words" and commercial speech.

Although Volokh's argument would predict that the "fighting words" doctrine established in Chaplinsky v. New Hampshire n145 would lead not only to a broadening of its own doctrinal category but also to the creation of new categories of unprotected speech, this has not happened in practice; indeed, although the Supreme Court has not reversed Chaplinsky, it has never subsequently upheld a conviction under the case's theory. n146 Thus, in Gooding v. Wilson, n147 when the Court addressed a conviction under a statute substantively identical to the one it upheld in Chaplinsky, it declared the statute unconstitutional under the overbreadth doctrine, even though the petitioner in that case had undeniably engaged in activity outside the First Amendment under the "fighting words" doctrine. n148

Similarly, although the Supreme Court held in Valentine v. Chrestensen n149 that commercial speech was unprotected speech, n150 subsequent **[*1179]** decisions have brought commercial speech within the protections of the First Amendment, n151 with the relaxed intermediate scrutiny of Central Hudson Gas and Electric Corp. v. Public Service Commission n152 giving way over time to greater and greater protection for commercial speech. As a result, the central issue of commercial speech doctrine has gradually but fundamentally shifted over the last twenty years from whether commercial speech should be protected at all to whether it warrants protection on a par with "core" political speech, as several members of the Court have argued. n153

It is certainly difficult to predict future events based upon trends from the past. But the robust protection that the courts have given to free speech suggests that refining categories of unprotected or partially protected speech is unlikely to lead to serious free speech problems down the road through any slippery slope mechanism. Indeed, the principal theoretical and practical difficulty at the intersection of speech and privacy is not a problem of protecting speech from

privacy, but of safeguarding some privacy protection under a juridical regime in which free speech always wins.

Although most privacy scholars believe that privacy rights are not extinguished by the First Amendment, the handful of such scholars who have disagreed explicitly with the First Amendment critique would also reject an approach to the problem that focuses on the boundaries of the First Amendment. Paul Schwartz and Daniel Solove concede that information disclosure rules raise First Amendment problems, but they believe that an adjusted right of data privacy can stand up to the First Amendment. Schwartz argues that nondisclosure rules can survive balancing against the First Amendment because they "help maintain the boundary between public discourse and the other realms of communication" and because "standards of fair information practices serve to safeguard deliberative democracy by shaping the terms of individual participation in social and political life." n154 Solove argues that in the context of information disclosure rules, privacy interests should be balanced against First Amendment rights. Although he considers **[*1180]** it tempting to exclude disclosures of private information categorically from the definition of "speech" under the First Amendment, Solove ultimately rejects this approach as "conceptually sloppy or even dishonest absent a meaningful way to argue that these examples do not involve communication." n155 According to Solove, "dealing with privacy issues by categorizing personal information as nonspeech is undesirable because it cloaks the real normative reasons for why society wants to permit greater regulation of certain communicative activity." n156 Solove argues that it is both preferable and more intellectually honest to engage in pragmatic, contextual balancing between speech and privacy. n157

Solove's and Schwartz's arguments are thoughtful, but I believe they grant too much ground to the First Amendment critique and ultimately may prove to be underprotective of privacy interests, particularly in the database context. First, to the extent these scholars share the same view of the boundaries of the First Amendment as the critics do, I have already addressed these objections. n158 Second, to the extent we disagree whether the sale of databases constitutes "speech" within the scope of the First Amendment, I argue below that under current doctrine, the sale or transfer of most commercial databases does not fall within the protections of the First Amendment.

Third, I doubt that Solove's balancing approach would provide meaningfully increased protection for privacy protection in the courts. Solove urges courts to depart from the current paradigms under which they balance privacy against the First Amendment - whether the individual is a public or private figure and whether the information is public or private - and to replace them with an approach focusing on "the relationships in which information is transferred and the uses to which information is put." n159 However, such an approach merely substitutes one vague set of criteria for another and risks an overcontextualized jurisprudence. As Solove concedes, "if social norms about the propriety of disclosures are too diffuse and contestable, then a law protecting against "improper' disclosures may become too unpredictable or even unworkable." n160 Solove's solution to this problem of "hyper-contextualism" is essentially the one put forth by Warren and Brandeis over 100 years ago - that courts can articulate the contours of murky rules like negligence on a **[*1181]** case-by-case basis. n161 I am skeptical that Solove's contextually pragmatic proposal would work significantly better than the categorically pragmatic method applied by existing jurisprudence. Solove's approach would, I fear, lead to inconsistent results through the processes of courts applying slippery standards on a case-by-case basis. In addition, any balance between the powerful First Amendment and a nuanced right of privacy is unlikely to protect much privacy at all.

Although some form of balancing is perhaps inevitable in the hard cases pitting privacy against the First Amendment, I believe it is not only important to separate out the easy cases from the hard cases, but also that an approach that treats private information differently is more consistent with the workable "categorical balancing" approach courts have taken in the First Amendment context since New York Times v. Sullivan. In the next part, I show how this approach works in practice.

III. Categorizing Privacy Rules Under the First Amendment

The previous part attempted to complicate the argument of the First Amendment critics that privacy rules necessarily regulate speech protected by the First Amendment. Because many privacy rules have nothing to do with information

flows, they have nothing to do with speech. And, as a conceptual matter, privacy rules regulating information flows are not necessarily within the scope of the First Amendment. In this part, I attempt to demonstrate more specifically why privacy rules will rarely, if ever, create a problem under the First Amendment.

Given the notorious slipperiness of the term "privacy," n162 it is necessary to impose some sort of order on the analysis that follows. Every information flow in the database context can be broken down into a series of stages, which are helpful categories to assess the different kinds of privacy rules that can apply to a transaction in personal information. Information is first collected by companies, then used to assemble databases, disclosed to companies wishing to use the information (either for marketing or for the creation of larger databases), and then often used as the basis for direct marketing, such as telemarketing or junk mail. Accordingly, possible regulations of information flows can be divided into four categories, corresponding to the four stages of information processing performed by the database industry: (1) rules governing the collection of **[*1182]** information, (2) rules governing the use of such information, (3) rules governing the disclosure of information, and (4) regulation of direct marketing.

This taxonomy makes, I believe, two significant contributions to the literature on information flows. First, looking at the problem in this way reveals that ordinary information collection and information use rules are not speech rules at all. Information disclosure rules are closer to speech, but in the commercial context they are usually outside the scope of the First Amendment. And while direct regulation of telemarketing is undeniably regulation of commercial speech within the scope of the First Amendment, current doctrine nevertheless permits quite extensive regulation of such speech. Second, regardless of whether individual or categorical sorts of privacy rules ultimately pass muster under the First Amendment, separating out the various types of privacy restrictions on the free flow of information allows us to take a careful look at the constitutional issues raised by four very different types of data privacy rules. In this regard, I hope that this taxonomy is a useful (and hopefully value-neutral) contribution to the discourse on information flows.

A. Information Collection Rules

Information collection rules govern the process of gathering data and assembling databases. They represent the legal regime covering the ways in which entities acquire information and specify when collection is permissible and when it is not. Examples include requiring a company to obtain a customer's permission before it makes a record of the customer's data, regulating the use of cookies to gather information on the Internet, and regulating or prohibiting the use of scanning devices to intercept telephone conversations or e-mails.

A wide variety of rules operate, directly or indirectly, to restrict access to information without raising First Amendment issues. Most fundamentally, generally applicable property and tort law prohibits information collection by separating the public sphere from the private. It is no defense to a claim of trespass for the trespasser to assert that he infringed the property rights of another to gain information. In addition to trespass, most states recognize the intrusion into seclusion tort, n163 one of the four "privacy torts" recognized **[*1183]** by William Prosser as having evolved out of Warren and Brandeis's Right to Privacy article. n164 The intrusion tort goes much further than trespass and imposes liability upon anyone "who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns ... if the intrusion would be highly offensive to a reasonable person." n165 Courts have applied this tort to mail tampering, n166 eavesdropping, n167 nonconsensual entry into homes, n168 sexual harassment, n169 repeated intimidating phone calls, n170 overzealous surveillance or "shadowing," n171 and sexual voyeurism. n172 Other sorts of information collection rules regulate unfair business practices such as industrial espionage. For example, the tort of misappropriation of trade secrets "protects a person's right to keep certain information "secret,' by providing a cause of action against anyone who misappropriates a reasonably protected secret." n173

[*1184] In addition to state tort law, certain forms of eavesdropping (including industrial espionage) n174 are also prohibited by federal law. The Electronic Communication Privacy Act (ECPA) prohibits the use of any "device" to intercept the contents of an aural conversation. n175 The ECPA has been held to outlaw, inter alia, secret tape recording of meetings, n176 hidden microphones, n177 the surreptitious eavesdropping on or recording of telephone conversations, n178 and the participation of telephone companies in illegal government wiretapping. n179 Furthermore,

many states also have statutes providing analogous civil actions n180 that in some instances offer more protection than the ECPA. n181

In the consumer context, information collection rules require disclosures by businesses and informed consent by consumers. These rules even outlaw commercial data gathering that is unfair or unconscionable. For example, fraud law generally governs the receipt of any thing of value (including personal **[*1185]** data) under false pretenses. n182 The use of fraud or other deceptive practices in obtaining consumer data could also constitute a violation of the Uniform Deceptive Trade Practices Act (UDTPA), n183 and would fall within the powers of the Federal Trade Commission (FTC) to deter and punish unfair trade practices under section five of the Federal Trade Commission Act. n184 Another important federal consumer protection law, the Fair Credit Reporting Act, regulates the assembly of credit reports, allowing, for example, employers to obtain credit reports for "employment purposes" only if the employee or potential employee first authorizes the collection in writing. n185

A variety of federal laws regulate information collection in the electronic context. Anti-hacking laws such as the Computer Fraud and Abuse Act (CFAA) impose criminal penalties on hackers by essentially exporting trespass law to the electronic world. For example, the CFAA imposes criminal punishment on anyone who "intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains ... information from any protected computer." n186 Federal wiretapping law, of which the ECPA is a significant part, also proscribes the intentional interception of the contents of an electronic communication such as an e-mail or telephone conversation, n187 without the consent of one of the parties to the communication, n188 and punishes a violation through both criminal n189 and tort law remedies. n190 The Children's Online Privacy Protection Act regulates the collection of information from children by web sites, imposing notice and express parental consent requirements. n191

[*1186] Finally, to the extent that web sites make representations about their information collection practices in their privacy policies, the FTC reviews these policies under its unfair trade practice jurisdiction. n192 One could imagine an expansion of FTC jurisdiction not only to require privacy policies, but also to dictate the substantive content of the trade practices that these policies address. n193 Similarly, as part of regulating the commercial relationship between customers and businesses, the law could require that businesses disclose their privacy policies with respect to the subsequent uses and disclosures of data they collect. It would be difficult to argue that regulating the commercial relationship in this manner implicates the First Amendment, even though one could imagine the disclosures as a kind of forced or compelled speech. Moreover, no one considers Securities Exchange Commission or Truth in Lending Act (TILA) disclosures or Food and Drug Administration labeling requirements to raise serious First Amendment issues.

My purpose in this discussion of information collection rules has not been to attempt to catalog them systematically, but rather to suggest their ubiquity. Information collection rules are a common feature of both common and statutory law. Unsurprisingly, these rules do not fall within the scope of the First Amendment under either current First Amendment doctrine or theory. These rules are of "general applicability," neither discriminating against nor significantly impacting the freedoms guaranteed by the First Amendment. n194 The paradigmatic case of a generally applicable law is the private property right against trespass, which does not implicate the First Amendment under well-established doctrine. Thus, in a line of cases involving protests in shopping centers, the Supreme Court has concluded that the First Amendment "has no part to play" n195 **[*1187]** in the general application of trespass law to protestors, because private landowners may, unlike the government, exclude speakers from their property for any reason, including their disagreement with the content of the speaker's message. n196

In at least two cases, however, rules governing information collection might be thought to cross into territory patrolled by the First Amendment. First, reporters engaged in newsgathering (a form of information collection) have argued that they have a First Amendment right under the Free Press Clause of the First Amendment to do so. This issue has been particularly salient of late in cases in which undercover investigative journalists have allegedly committed torts in their pursuit of a story. n197 Although mindful of the importance of a free and vigorous press corps, courts have declined to grant the press an immunity from lawbreaking in pursuit of a story, even a newsworthy one. n198 For example, in the high-profile Food Lion, Inc. v. Capital Cities/ABC, Inc., n199 the Fourth Circuit held that investigative

journalists who obtained jobs at a grocery store under false pretenses in order to videotape and publish suspected sanitary abuses trespassed and violated the duty of loyalty under state law. n200 Although the law is unclear with respect to whether fraudulently induced consent to enter onto land is valid, n201 and although the press may get the benefit of the doubt at the margins, n202 no case recognizes a First Amendment investigative privilege that provides immunity from generally applicable property and tort rules like trespass. n203

[*1188] The Supreme Court's First Amendment jurisprudence makes clear that even media defendants collecting newsworthy information enjoy no privilege against the application of ordinary private law. Indeed, such rules do not trigger the application of heightened First Amendment scrutiny unless they single the press out for special unfavorable treatment. n204 The Court recognized this principle in Branzburg v. Hayes, n205 when it noted:

It would be frivolous to assert ... that the First Amendment, in the interest of securing news or otherwise, confers a license on either the reporter or his news sources to violate valid criminal laws. Although stealing documents or private wiretapping could provide newsworthy information, neither reporter nor source is immune from conviction for such conduct, whatever the impact on the flow of news. n206

Similarly, in Cohen v. Cowles Media, n207 the Court held that "the press may not with impunity break and enter an office or dwelling to gather news." n208 The Court reaffirmed this principle most recently in Bartnicki v. Vopper, n209 expressly quoting its validation in Branzburg of generally applicable information collection rules. n210

The Court's public law cases imply a similar reasoning. In the Pentagon Papers case, some members of the Court suggested that although the prior restraint doctrine prevented the government from halting the publication of the secret report, the case might have been different had the reporters come before the Court on criminal charges for illegally acquiring classified government documents. n211 Similarly, in Wilson v. Layne, n212 the Supreme Court held that police who brought newspaper reporters into a private home during a search pursuant to a valid warrant nevertheless violated the Fourth Amendment. The newsmen were in effect trespassers, and their media status was deemed **[*1189]** irrelevant to the illegal nature of their presence. These cases embody the principle that ordinary information collection rules create no constitutional problems, even as applied to the press, as such rules form the background against which private action plays out. They also demonstrate that there are few, if any, problems with drawing lines in this context between activity that falls within the scope of the First Amendment (for example, publishing a newspaper) and activity that does not (for example, trespass, even for the purposes of gathering information).

Second, even neutral rules regulating conduct such as information collection fall within the scope of the First Amendment when they have a substantial effect upon "conduct with a significant expressive element." n213 In such cases, the Court applies intermediate scrutiny consistent with its content-neutral speech restrictions jurisprudence. n214 One can imagine science fiction-style hypotheticals that would bring information collection rules within this doctrine - for example, a law forbidding the keeping of records or outlawing cameras. But such laws would probably violate the First Amendment under the overbreadth and vagueness doctrines as well, or might even fail rational basis review without calling into question the undeniable constitutionality of ordinary information collection rules. n215

The larger point to be drawn from these counterexamples is not that ordinary information collection rules raise First Amendment issues. To the contrary, even reporters have had a difficult time asserting a First Amendment privilege against neutral information collection rules. n216 Information collection by nonmedia entities raises even fewer First Amendment concerns than does newsgathering by the press. And if there are essentially no First Amendment problems with subjecting the press to the basic principles of generally applicable laws, privacy rules regulating data collection by nonmedia entities fall outside the scope of the First Amendment as well. Thus, because reporters cannot claim a First Amendment privilege to gather information in **[*1190]** disregard of tort and property law, it is difficult to envision businesses mounting a colorable free press challenge to consumer-protective privacy rules regulating commercial data transactions. This is particularly true for rules that regulate the commercial relationship between consumers and

businesses. In sum, because there are no First Amendment problems with using generally applicable property and tort law to separate the private sphere from the public sphere, the First Amendment critique is simply inapplicable to information collection rules.

B. Information Use Rules

The second category of information flow regulations are restrictions on information use placed on recipients of data. Information use is an analytically distinct activity from information collection, but it is similarly unproblematic from a First Amendment perspective. Information use rules regulate the ways in which data about individuals can be processed, applied, or otherwise used by a person or organization. This category of rules does not include the transfer, sale, or disclosure of the data to third parties. n217 Information use rules that are relevant to the data privacy debate include the so-called "secondary use prohibition": the requirement that data collected for one purpose may be used for that purpose only, absent consent. n218 For example, the secondary use prohibition might operate to bar an Internet Service Provider from using the fact that a person visits political fringe or sex-oriented web sites from using that information to send them personalized advertisements. Alternatively, a use rule might prevent a private business that collects my personal information as part of a transaction from including that information in a customer marketing database. n219 Other sorts of information use rules include a prohibition on the use of social security numbers to organize, combine, assemble, and process consumer data profiles more easily. n220

As with information collection rules, information use rules permeate the common law and statute books of all jurisdictions. n221 For example, professional ethics rules prohibit lawyers from using client information for any purpose **[*1191]** unrelated to the client's interests. n222 It is also a violation of numerous federal and state antidiscrimination laws to use the fact that a person is a member of a protected class to deny them equal treatment, or to take any one of a variety of other actions. n223 Similarly, the federal Fair Credit Reporting Act places a wide variety of restrictions on the use of consumer data contained in credit reports, including limiting uses to an enumerated list, including credit review, insurance underwriting, and employment purposes. n224 Employers using credit reports for employment purposes are also prohibited by the Act from any use inconsistent with applicable equal opportunity employment rules. n225 Trade secret law prohibits the use or disclosure of another's trade secrets. n226 Similarly, federal patent law prohibits the use of information contained in someone else's patent to build the invention described in that patent. n227 States place use conditions on social security numbers n228 and information obtained from their motor vehicle records, n229 while federal law places similar use restrictions on census data. n230

[*1192] The Electronic Communications Privacy Act also imposes a use restriction on information that is obtained in violation of its information collection prohibition on intercepting the contents of electronic, wire, or aural communications. n231 ECPA's information use prohibition has been upheld in a variety of contexts involving different uses of information, including the use of intercepted communications from a commercial rival, inter alia, to create a competing product, n232 to read a document or listen to a recording obtained as a result of illegal interception, n233 to invest in securities, n234 to take adverse employment actions against employees or subordinates, n235 to use in family or criminal court proceedings, n236 to use in criminal or administrative investigations, n237 and possibly to use as the basis for blackmail. n238

Information use rules, just like information collection rules, are generally held to be outside the scope of the First Amendment under current doctrine. In Bartnicki v. Vopper, the Supreme Court assessed the First Amendment implications of the Wiretap Act's prohibition of the use or disclosure of intercepted communications. n239 The Court drew a sharp distinction between the use of a communication under 2511(1)(c) of the Act and its disclosure under 2511(1)(d), reasoning that while disclosures of information could certainly constitute speech, "the prohibition against the "use' of the contents of an illegal interception in 2511(1)(d) ... [is] a regulation of conduct." n240 As a content-neutral regulation of conduct, ECPA's information use rule would fall outside the scope of the First Amendment unless, like the information collection rules discussed above, it had a substantial effect upon expressive activity. As the Court strongly implied in Bartnicki, virtually all of the activities that prior cases have held to constitute a "use" of intercepted information **[*1193]** therefore would be constitutionally unproblematic. n241 I discuss the disclosure issue

(and Bartnicki) in Part II.D, but for present purposes, it is important to note the Court's clear distinction between regulating the use of information - nonspeech conduct largely outside the scope of the First Amendment - and regulating the disclosure of information that in some circumstances (like the radio broadcast at issue in Bartnicki) may regulate speech.

The issue of whether an information use rule violated the First Amendment was assessed peripherally in U.S. West, Inc. v. FCC, in which the telephone companies sought to use customer information they had received for one purpose (providing phone service) for an unrelated purpose (marketing). Laurence Tribe argued on the telephone companies' behalf that their processing of personal data was speech entitled to full First Amendment protection. n242 The Tenth Circuit accepted this version of the First Amendment critique and partially agreed. Perhaps unwilling to deal with Tribe's somewhat befuddled argument that the use and processing of data within a company was speech entitled to greater protection than commercial speech, the court concluded that the regulations as a whole placed a restriction on U.S. West's "targeted speech to its customers ... for the purpose of soliciting those customers to purchase more or different telecommunications services." n243 U.S. West's commercial speech rights were therefore unduly burdened. n244 The use of the information, the court asserted, was "integral to and inseparable from" the commercial solicitation. n245 Applying the Central Hudson test for commercial speech restrictions, the court thus invalidated the regulation by determining that the opt-in requirement did not directly and materially advance the state interest in protecting consumer privacy, n246 and that the regulation was not narrowly tailored because it failed to consider an available, less-restrictive alternative. n247 **[*1194]** The court also questioned, without deciding, whether a vague interest in protecting consumers from the embarrassment of the disclosure of their data amounted to a substantial government interest. n248

The Tenth Circuit's reasoning appears wrong under existing law. The FCC rules allowed the telephone companies to advertise to all of their customers, prohibiting them only from using the information to target the advertisements without approval. The rates were thus an ordinary example of a secondary use prohibition that is common to codes of fair information practices, none of which have been held to violate the First Amendment. n249 The only relevant burden placed on the telephone companies was on their ability to use, absent advance customer approval, the information they collected from those customers in the course of their commercial relationship to "target" advertisements to them - that is, to select those most likely to be receptive to such advertisements. n250 The rules were thus not a regulation of speech at all, but rather a regulation of information use - the business activity of deciding to whom to market products. The only burden placed upon the telephone companies was that their advertisements had to be sent to all of their customers, thus making those advertisements less cost-effective. Conduct (and economic conduct at that) was thus all that was regulated, and the Supreme Court has made clear that conduct can be regulated without implicating the First Amendment. The U.S. West example is thus but another instance of the First Amendment critique persuading courts to ask the wrong questions about the First Amendment - that is, to skip the scope question and ignore whether the activity being regulated is really speech within the scope of the First Amendment.

In sum, under established precedent, the conduct of using information, like the conduct of gathering information, can be regulated through generally applicable laws without implicating the First Amendment in most cases, because information use rules generally regulate nonexpressive conduct rather than speech.

C. Information Disclosure Rules

The third category of information restrictions implicated by fair information practices are restrictions on the disclosure of personal information. **[*1195]** Information disclosure rules regulate the ability of persons in possession of information to communicate, sell, or otherwise transfer that information to others. Information disclosure rules can take a variety of forms, including evidentiary privileges, Warren and Brandeis's tort of disclosure of private facts, video rental privacy protection, and duties of confidentiality and nondisclosure placed upon lawyers and financial advisers.

American law is replete with legal obligations placed on one person not to disclose information about another. While parties are of course generally free to create contracts that regulate their ability to disclose information, n251 public and private law regimes impose numerous mandatory duties of confidentiality that go beyond the contract of the

transacting parties to prevent the disclosure of information through speech or other means. For example, doctors, n252 lawyers, n253 and other professionals owe their clients duties of confidentiality, and can be punished through administrative and tort law remedies if they breach these duties by telling confidences to third parties. These duties of nondisclosure are buttressed by analogous evidentiary privileges, which give clients the ability to prevent their lawyers n254 and doctors n255 from speaking against their interests, presumably even when the content of the testimony would be quite newsworthy. Evidence law goes further and grants testimonial privileges to present and former spouses, n256 psychotherapists, n257 and others. n258

In the commercial context as well, many legal rules impose duties of nondisclosure or confidentiality. For example, agency law imposes a general **[*1196]** duty of confidentiality upon agents not to disclose their principal's information. n259 State trade secret law enforces a mandatory regime of nondisclosure that prohibits, inter alia, the disclosure of trade secrets to competitors. n260 Furthermore, some states place nondisclosure rules on social security numbers. n261

Federal statutory law imposes numerous duties of confidentiality under the federal commerce power. The federal Economic Espionage Act also prohibits the disclosure, sale, or receipt of trade secrets, and punishes individual violations with up to fifteen years imprisonment and institutional violations with fines of up to $ 10 million. n262 Federal securities, antitrust, and labor law impose numerous duties of nondisclosure of truthful information upon corporations. n263 Recent federal statutes place nondisclosure obligations upon banks with respect to customer information, n264 and upon hospitals with respect to patient medical information. n265 Federal law also imposes duties of confidentiality upon cable companies and video stores, charging them with keeping confidential the videos watched by their customers. n266 ECPA provides that the disclosure of an intercepted communication is a separate violation from the interception and use of that communication. n267 Another provision of federal wiretapping law places a duty of confidentiality upon Internet Service Providers with respect to the content of e-mails sent and received by their customers. n268

Most commercial nondisclosure or confidentiality rules have never been thought to fall within the scope of the First Amendment's protection. Like other commercial regulations, these rules are properly assessed under rational **[*1197]** basis review. n269 However, a few information disclosure rules undeniably restrict speech within the scope of the First Amendment in some circumstances - for example when the tort of publication of private facts is applied to a newspaper that wishes to publish information of public concern that it obtained lawfully. n270 Indeed, much of the historical conflict between the privacy tort and the First Amendment has come as a result of litigation over the ability of the media to publish private facts it had received about subjects it felt to be newsworthy. The Supreme Court has consistently upheld the right of the established media to publish even the most intimate private facts regardless of any countervailing privacy interest. n271 For example, in Florida Star v. B.J.F., n272 the Supreme Court held that the First Amendment protected a newspaper that had published the name of a rape victim from liability under a privacy tort action, even though a government employee had violated agency policy by disclosing the name to the reporter. n273 Unsurprisingly, the First Amendment critics rely heavily upon this line of cases to argue that "while privacy protection secured by contract is constitutionally sound, broader information privacy rules are not easily defensible under existing free speech law." n274 Accordingly, First Amendment critics assert that only market-based solutions to the database problem - that is, contract, self-regulation, or privacy-enhancing technological solutions - are cognizable options given the dictates of the First Amendment. n275

The contemporary First Amendment critique is part of a larger tradition of scholarship and jurisprudence regarding the tension between the First Amendment and the classic formulation of the privacy tort. Indeed, to understand the critique properly, as well as to perceive some of its core **[*1198]** assumptions and limitations, a brief exploration of its origins is helpful. Although American law has long protected various aspects of privacy (including what we today would call data privacy), n276 modern thinking about the right of privacy is often traced to Warren and Brandeis's privacy article, in which their concern was not primarily data privacy, but rather media use of private information. n277 In particular, Warren and Brandeis sought to use common law tort rules as a possible remedy for the collection and publication of personal details about famous persons by newspapers and magazines. n278 Although such a clear attempt to regulate the publication of truthful information by the press would appear to be in direct tension with modern First

Amendment doctrine, the Supreme Court at that time had yet to begin its project of giving the First Amendment preemptive force over tort law. n279 In addition, the tort of privacy was itself immature, with early cases largely involving the right of individuals to protect themselves against the commercial misappropriation of their likeness by businesses, n280 a context removed from both the principal concern of Warren and Brandeis and from the core of First Amendment protection. The privacy torts as we known them today were given their modern formulation as a result of the work of William Prosser in the period immediately after the Second World War. n281 Prosser revised and restated the privacy tort into four separate strands: "appropriation privacy"; intrusion privacy, which dealt with intrusions into the home or personal possessions; unauthorized public disclosure of "private" information; and the tort of "putting the plaintiff in a false but not necessarily defamatory position in the public eye." n282 Prosser's categorization of the third strand - the tort punishing the publication of truthful but private information - rejuvenated the argument of Warren and Brandeis. Indeed, Prosser expressly credited Warren and Brandeis with the "origins" of the privacy tort, n283 even though he had done almost as much to establish it as a recognized and refined body of **[*1199]** law. n284 Prosser's taxonomy of the tort of privacy in the various editions of his treatise between 1941 and 1960 gave order to the various strands of doctrine at a time when the Supreme Court was beginning to address the role of the First Amendment in tort law. Prosser and others warned of the tension between the First Amendment and the tort of publication of private information, n285 and the Supreme Court seemed to confirm this warning in its line of privacy cases, in which the private plaintiffs lost and the media won. n286 As a result, there is an enormous literature discussing whether the post-New York Times v. Sullivan First Amendment dooms the disclosure tort completely. n287

In light of these cases, scholars - and privacy scholars in particular - have been quite gloomy about the prospects of privacy. However, such a prognosis tends again to confuse the outcomes of a handful of reported cases with the full extent of the law in actual practice. n288 As noted above, while privacy and speech have been in famous conflict involving the nondisclosure tort as applied to newspapers, privacy and speech have coexisted harmoniously throughout the overwhelming majority of nondisclosure rules, which have never raised constitutional issues. n289 The Supreme Court may have held in favor of press immunity from privacy rules in the Florida Star/Bartnicki line of cases, but it does not follow from these cases that nondisclosure rules applied in other circumstances - for example, to nonpress entities engaged in ordinary commercial activity - are constitutionally suspect. First, the Court has made quite clear in each of these cases that its ruling was narrow. n290 Second, because of the importance of both privacy and the First Amendment, the Court has repeatedly declined to address the issue of "whether truthful publication may ever be punished consistent with the First Amendment." n291 Third, all of these cases involve media defendants publishing allegedly newsworthy facts, but the vast majority of **[*1200]** nondisclosure rules do not involve media defendants or newsworthy information, although a few high-profile cases may be produced from time to time.

Where, then, do nondisclosure rules fall under current doctrine? If the privacy tort is dead, why is our law filled with nondisclosure rules that we find constitutionally unproblematic, and, indeed, have never envisioned to fall within the scope of the First Amendment? As Schauer might put it, why have we not perceived the constitutional salience of other nondisclosure rules like the attorney-client privilege or the Video Privacy Protection Act? Some privacy scholars have proffered the concept of "private speech" as a justification for sustaining nondisclosure rules against the First Amendment. n292 Building upon Warren and Brandeis's distinction between matters of public and matters of private interest, n293 these scholars suggest that courts should develop a category of speech that is "private" or at least not a matter of public concern. n294 By so doing, these scholars hope to rejuvenate the tort of disclosure of private facts to make it applicable in at least egregious cases against media defendants. Although the Supreme Court has declined to hold categorically whether truthful speech on a matter not of public concern may ever be restrained consistent with the First Amendment, n295 the "private speech" theory has some support in First Amendment doctrine. For example, in Dun & Bradstreet, Inc. v. Greenmoss Builders, Inc., n296 a plurality of the Court noted in a private-figure trade libel case that speech not on matters of public concern receives "less stringent" First Amendment protection. n297 Even in Bartnicki v. Vopper, a case received gloomily by most privacy scholars, n298 the Court strongly implied that the First Amendment could only defeat privacy if the speech being regulated was "unquestionably a matter of public concern." n299 However, such a theory is mostly unhelpful to the protection of the vast majority of consumer data privacy laws for a couple of reasons. First, by attempting to justify **[*1201]** privacy rules against media disclosures, it lumps the

easy case of consumer privacy rules with the hard case of privacy against the press. In so doing, it necessarily concedes that privacy rules are speech rules. Second, requiring courts to determine whether speech is "public" or "private" would be incredibly difficult and likely lead to indeterminate and inconsistent outcomes.

It is not necessary to develop a new jurisprudence of private speech to sustain consumer privacy rules, as existing doctrine is more than adequate to protect such rules without implicating the First Amendment. With the historical context of privacy and speech in mind, I believe that two additional factors help explain not only why consumer privacy rules have not been thought to implicate the First Amendment, but also why such rules do not in fact do so. First, many forms of nondisclosure rules are enforceable through express or implied contracts. Second, generally applicable law can operate to create a kind of "information contraband" n300 to which nondisclosure obligations can be attached without encroaching upon the scope of the First Amendment.

1. Contract-based Nondisclosure Rules

Contract as a basis for nondisclosure rules is an uncontroversial proposition in the privacy literature, even among the First Amendment critics. n301 Two parties can create an information nondisclosure contract that the courts will enforce, even if the party agreeing to keep the information secret is a newspaper and the information is newsworthy. The Supreme Court has made clear that there does not even need to be an enforceable contract to hold the media liable for damages under such circumstances. In Cohen v. Cowles Media Co., n302 the Court upheld the application of promissory estoppel principles to allow a plaintiff to recover against a newspaper that had broken its promise of confidentiality to him. The plaintiff had disclosed embarrassing information relating to the state lieutenant governor's prior criminal record in exchange for the newspaper's promise to keep his identity secret. The newspaper then published the allegations along with the plaintiff's name. Writing for the Court, Justice White held that the state's "law of general applicability" of promissory estoppel could be enforced against the newspaper because "generally applicable laws do not offend the **[*1202]** First Amendment simply because their enforcement against the press has incidental effects on its ability to gather and report the news." n303

Eugene Volokh reads Cohen as merely establishing the principle that the First Amendment does not generally prohibit the enforcement of express or implied speech-restricting contracts against the press. n304 Volokh acknowledges that this principle allows government to impose statutory default nondisclosure rules upon a variety of relationships in which ordinary social conventions include an expectation of confidentiality, including relationships between consumers and doctors, lawyers, and even video stores at the outer limits. n305 However, he suggests that this general principle is subject to two significant limitations. First, it only allows people to restrict the speech of persons with whom they have a contract, and it does not cover third parties who are outside the scope of contractual or quasi-contractual privity. n306 Second, it does not justify mandatory government-imposed nondisclosure rules that the parties cannot waive. n307

Volokh's category of unobjectionable speech restrictions based on a contract theory is significantly broader than it might appear at first blush. First, his use of contracts as a limiting principle is unpersuasive on its own terms. Volokh concedes that implied contracts are also outside the First Amendment. Viewing "implicit" contracts, broadly defined, as falling outside the scope of the First Amendment thus includes not only contracts that can be implied from the circumstances surrounding a transaction, but also default statutes setting up the terms of a transaction but giving parties the option of bargaining around the rule. n308 Volokh also admits that the government can supply default rules to relationships that social convention considers confidential, and he suggests that the U.S. West case was incorrectly decided on this basis. n309 However, this additional concession gives away most of the game, because virtually all nondisclosure rules outside the media context tend to reinforce implicit social conventions of confidentiality - for example, as Volokh recognizes, the Video Privacy Protection Act reflects such a social expectation in requiring video rentals to be kept secret. n310 But once the law can modify a relationship of **[*1203]** this sort, it is hard to see where such a principle would stop, other than to render all default rules constitutional. Moreover, to the extent that law can reinforce social norms, a privacy rule applied to an area where there is no existing social convention of confidentiality could, over time, create new such norms. For example, scholars have argued that this is exactly what FTC regulation of

privacy policies achieves in the Internet context. n311 It would also seem to follow under this theory that terms should be able to be supplied to constructive "relationships" as well. Just as the law unremarkably can impose duties of confidentiality upon a lawyer when the client reasonably believes that an attorney-client relationship exists, other duties could be prescribed to regulate the ways in which profiling and marketing companies use sensitive customer data, including massive profile databases. Thus, Volokh's acceptance of implied contracts seems to permit the government to supply a whole range of default rules to any relationship involving privacy that the government thinks reasonable to regulate.

Volokh's second limiting principle is that while default rules may be permissible, mandatory rules violate the First Amendment. This argument is also unpersuasive. First, Volokh offers little justification for the claim that mandatory rules are somehow different than default rules from a First Amendment perspective, other than to note that the essence of contract is consent, which the Court in Cohen recognized. n312 But other regimes operate to supply mandatory nondisclosure rules without falling within the scope of the First Amendment. For example, trade secret law places a mandatory obligation on those who come across trade secrets not to disclose them to others, even if the person who comes across the secret has no relationship to the trade secret holder. n313 Similarly, contract law supplies a whole host of mandatory terms in the consumer context in which there is reason to believe that diminished capacity exists; yet these terms do not raise constitutional issues. n314 This includes, for example, the legislative prohibition of certain types of transactions where the bargain itself is thought to be unconscionable. n315 In analogous contexts involving consumer privacy, then, mandatory rules should be equally unproblematic - for example, the Children's Online Privacy Protection Act, which does not give children the right to waive their privacy rights and **[*1204]** prohibits companies from collecting information about children without parental consent. n316 Similarly, scholars have noted that many consumers do not understand the technology of the Internet, the legal language of privacy policies, or the nature of the trade in personal information. This ignorance leads to a form of "privacy myopia," in which consumers sell their data too frequently or too cheaply. n317 For example, some consumers who care deeply about privacy nevertheless sell their information bit by bit for frequent flier miles. n318 If a legislature were to conclude that consumers were behaving myopically in information transactions, it could also conclude that consumers are incapable of waiving their privacy rights in the context of such a transaction, just as a legislature might police standard-form contracts or consumer credit transactions in the offline context. In all of these examples, economic policing of the risk of unconscionability would be assessed under the rational basis review reserved for economic regulation generally. n319

Contract thus provides a quite expansive rationale for regulating consumer privacy transactions outside the scope of the First Amendment. Particularly when we recognize the enormous power that legislatures possess to structure and regulate the terms of economic transactions, the regime of contract law grants policymakers a wide variety of regulatory tools, including the power to supply both default and mandatory terms to transactions. Such instances of contractual commercial regulation are well outside the scope of the First Amendment.

2. Creation of Nondisclosure Rules via Generally Applicable Law

The promissory estoppel remedy in Cohen is certainly a broader theory of liability than contracts at law. But the remedy is still essentially a contractual one, albeit one that imports concepts of reliance and equity. n320 Another theory under which a wide variety of nondisclosure rules can be justified outside the scope of the First Amendment is the related concept of "generally applicable law." Cohen did not rest for the theory that only contract law can uniquely insulate speech restrictions from First Amendment difficulties. Rather, it stood for the much broader theory that a larger category of generally applicable laws do not violate the First Amendment, at least insofar as they **[*1205]** do not place a significant burden upon protected, expressive conduct. n321 In other words, Cohen suggests that "generally applicable laws" comprise a broader category, of which contract is but one doctrinal strand of several. Such a conclusion is confirmed by several other cases. For example, in Seattle Times Co. v. Rhinehart, n322 the Court held that a protective order placed on a newspaper involved in litigation could be applied validly to the newspaper to prevent it from disclosing the contents of newsworthy information it learned as a result of the discovery process. Indeed, extrapolating from Rhinehart, Lucas Powe - no enemy of the press, to be sure - has argued that "if the press broke into a building and

pillaged files - or planted bugs - and later published, then the publication could be taken as insult upon injury," and the press could be subjected to liability for publication of the wrongfully obtained information. n323 Such a principle is fully consistent with Bartnicki and the other cases in which the Court invalidated public laws and tort actions that interfered with the media's First Amendment rights, because each of those cases held that the media had lawfully obtained the published information. n324 Read together, these cases suggest that information disclosure rules that are the product of generally applicable laws fall outside the scope of the First Amendment. If information is received by an entity in violation of some other legal rule - whether through breach of contract, trespass, theft, or fraud - the First Amendment creates no barrier to the government's ability to prevent and punish disclosure. This is the case even if the information is newsworthy or otherwise of public concern. n325 In this regard, the information is a kind of contraband, and traffic in it (at least by those with unclean hands) can be regulated.

[*1206] Volokh argues that such a principle could be used to justify troubling laws in the name of "privacy," such as a law providing that all questions by reporters would carry with them an implicit promise of confidentiality, or

a law providing that people who buy a product implicitly promise to give the seller equal space to respond to any negative article they publish about the product, unless the seller consents in writing after being given full disclosure of the true purpose for which the product is being bought. n326

However, unlike the law upheld in Cohen, neither of these examples is really a law of general applicability. Because both laws would have a significant impact upon expressive activity on matters of public concern, they would likely trigger intermediate scrutiny under current doctrine. n327 Additionally, because the media confidentiality law singles the media out for special unfavorable treatment, it would be subjected to strict scrutiny. n328 Both examples are thus a long distance from the ordinary nondisclosure rules that permeate American law.

Ordinary nondisclosure rules (even mandatory ones) are less threatening to First Amendment values than the speech restriction upheld in Cohen for another reason. Cohen did not just involve information that was unlawfully obtained, but also undeniably newsworthy information that was disseminated by the press, the latter of which the Court has long recognized as filling an important social function. From a First Amendment perspective, no such equivalently important social function is provided by database companies engaged in the trade in personal data. Indeed, a general law regulating the commercial trade in personal data by database, profiling, and marketing companies is far removed from the core speech protected by the First Amendment, and is much more like the "speech" outside the boundaries of heightened review. n329

[*1207] Thus, even though some information disclosures can be viewed as speech within the scope of the First Amendment, information disclosure rules regulating nonnewsworthy information or disclosures of information that was not lawfully obtained (regardless of whether it is newsworthy or not) are, as a general matter, outside the scope of the First Amendment and are thus constitutionally sound.

D. Regulation of Direct Marketing

Regulation of direct marketing - whether junk mail, a telemarketing call, unsolicited spam e-mails, or some other means - is undeniably regulation of speech. Indeed, it may seem odd even to categorize a telemarketing call as the regulation of an information flow, except insofar as the information flowing in this case is an invitation to purchase a product. However, because this issue is tied up in the database problem, in the First Amendment critique and in the larger free speech and database privacy debate, it is worth some examination, if only to show the ways in which it differs from the other stages, and to demonstrate how the First Amendment critique is just as unpersuasive in this context as in the others.

A telemarketing call is an example of the final and most intrusive stage of the database problem, occurring after the

collection of personal data by a profiling company, the use of that data to determine which consumers best fit a target profile, and the disclosure of the profile to a telemarketing company that wishes to purchase it. Unlike those previous stages, a telemarketing call is undoubtedly "speech" within the scope of the First Amendment. As discussed above, current doctrine answers the protection question by treating commercial speech restrictions with intermediate scrutiny by applying the four-part Central Hudson test, although the trend over the past two decades seems to be that the test is being applied with more heightened scrutiny. n330 The First Amendment interest in telemarketing is thus greater than the corresponding interest in information collection, use, and disclosure rules.

On the other hand, the privacy interests at stake in the telemarketing context are not only stronger and more intellectually coherent than in the **[*1208]** collection, use, and disclosure contexts; they are also more likely to resonate with a court. Although scholars have struggled to define "privacy," there is a consensus that the general term "privacy" encompasses three separate "clusters." n331 "Substantive" or "decisional" privacy is the constitutional right to make certain fundamental decisions free from government scrutiny or interference. Cases like Roe v. Wade n332 and Griswold v. Connecticut n333 embody this privacy cluster. "Residential privacy" refers to the privacy interest individuals have in their homes against unwanted surveillance or interference by government, businesses, or other individuals. n334 "Data privacy" (also known as "information privacy") refers to the notion that the rights of individuals are threatened by detailed private-sector databases containing profiles of their preferences, including information about which consumer products they use, as well as potentially embarrassing information about their health, political views, or sexual predilections. n335

While telemarketing implicates data privacy, it also implicates residential privacy, because telemarketing disturbs individuals in the enjoyment of their homes. And unlike data privacy, which is a poorly articulated right, residential privacy is a robust right of constitutional magnitude that can hold its own against free speech. Indeed, the Supreme Court has long been solicitous of residential privacy as a substantial regulatory and societal interest, not just in the Fourth Amendment context, n336 but also as a bulwark supporting other constitutional privacy rights. n337 And whereas the data privacy right embodied in the disclosure tort has traditionally failed to compete with the First Amendment in cases in which the two rights have come into conflict, the privacy interests inherent in the home have long been able to defeat even core First Amendment speech. As early as 1943, the Supreme Court reaffirmed the right **[*1209]** of homeowners to exclude unwanted speakers from their property, n338 although it invalidated a municipal ordinance prohibiting door-to-door distribution of handbills. The Court was more explicit in Frisby v. Schultz, n339 in which it declared:

> One important aspect of residential privacy is protection of the unwilling listener. Although in many locations, we expect individuals simply to avoid speech they do not want to hear, the home is different... . [A] special benefit of the privacy all citizens enjoy within their own walls, which the State may legislate to protect, is an ability to avoid intrusions. Thus, we have repeatedly held that individuals are not required to welcome unwanted speech into their own homes and that the government may protect this freedom. n340

As a result, when the Court in Rowan v. United States Post Office Dep't n341 assessed a First Amendment challenge to the constitutionality of a federal law allowing homeowners to prevent companies from sending them sexually explicit junk mail and to have their names removed from the mailing lists, it upheld the law on residential privacy grounds.

It should therefore be no surprise that even the Tenth Circuit - which had not previously held data privacy in high regard n342 - recently upheld the FCC's Do-Not-Call regulations of telemarketers against a First Amendment challenge. Although the district court in that case had been swayed by the First Amendment critique, n343 the Court of Appeals, relying on the tradition of residential privacy, upheld the Do-Not-Call Registry n344 against the same Central Hudson challenge that had felled the FCC's data privacy regulations in the U.S. West case. n345 Indeed, other Supreme Court precedent suggests that the intrusiveness of telemarketing makes for a cognizable harm that can be regulated under the First Amendment, despite the fact that telemarketing is commercial speech. n346

[*1210] * * * * My argument to this point has hopefully demonstrated that the First Amendment critique rests on both an unpersuasive conception of the structure of First Amendment protection, and a cramped reading of the sorts of information regulations that are reconcilable with our commitment to free speech. The previous part has suggested that ordinary doctrinal tools can be used to demonstrate the constitutionality of a wide variety of privacy rules both applied to the database context and other contexts. However, simply because the law is a certain way does not mean that it should remain so. In the next part, I develop a normative account explaining why I believe that the interpretation of both First Amendment and data privacy law that I have sketched up to this point is in fact superior to the account put forth by the First Amendment critics.

IV. The Perils of Volokhner

Although information flows can be regulated in the consumer privacy context under current doctrine, the First Amendment critique has nevertheless attracted many adherents. Despite its simplicity (or perhaps because of it), scholars and judges tend to find it persuasive. After all, given the central importance of the First Amendment in American political and legal culture, who wants to be against the First Amendment, in any context? n347 I have suggested that one of the dangers of the First Amendment critique is that it represents a constitutionalization of data privacy rules, placing a thorny and tremendously important social issue beyond the regulatory authority of elected legislatures. In this respect, the First Amendment critique can be located within the broader strand of First Amendment thought that believes, drawing upon libertarian theory, that the First Amendment guarantees not just freedom of speech for individuals, but also for business interests, and that many economic regulations conflict with the First Amendment. But free speech doctrine is malleable and often indeterminate, and although the First Amendment critique is shaky under current First Amendment doctrine, it is neither absurd nor lacking in facial appeal. In light of this observation, it is essential to articulate justifications against both the constitutionalization of information policy and the stretching of First Amendment doctrine into areas where it does not fit.

[*1211] In this part, I explore some of the ramifications of the First Amendment critique for free speech and rights jurisprudence generally. I have argued that much of the confusion in the law at the intersection of privacy rights and the First Amendment comes from the conceptual murkiness at the core of both privacy law and (counterintuitively) the First Amendment itself. First Amendment critics are quick to apply seemingly applicable or analogous doctrinal tests to privacy rules, but are less able to supply jurisprudential values advanced by the critique other than a vague notion of the "freedom of information." In fact, when viewed from the perspectives of both privacy law and First Amendment law, the First Amendment critique of data privacy rules threatens serious and pernicious jurisprudential consequences.

In Part IV.A, looking at the issue from the perspective of privacy law, I examine the broader implications of the First Amendment critique and its "freedom of information" principle for information policy. In so doing, I assess the argument that the First Amendment critique is merely Lochnerism in another guise. I conclude that although there are parallels between the First Amendment critique and the traditional understanding of Lochner, recent scholarship by legal historians has complicated this sort of claim, revealing that Lochner in practice was not as doctrinally illegitimate as its critics have charged. Nevertheless, to the extent that the First Amendment critique resembles the traditional view of Lochner, this remains a fairly significant criticism, suggesting that the First Amendment critique is out of step with many basic assumptions about the First Amendment. In Part IV.B, I look at the critique from the other side - from the perspective of First Amendment law. I argue that examining the revisionist intellectual history of Lochner reveals the real jurisprudential threat of the movement of which the First Amendment critics are a part - an obliteration of the distinction between economic and political rights that represents the core of modern constitutionalism.

A. The First Amendment Critique and "Freedom of Information" as Lochner

Although much is contested at the intersection of data privacy and the First Amendment, one thing at least is clear: First Amendment critics assert that because data privacy rules violate the First Amendment, the regulation of data privacy should be placed beyond the scope of normal regulatory policy and politics. They may couch the constitutional mandate apologetically because of the need to protect other, more important values, n348 or they may assert **[*1212]**

unapologetically that freedom of information is both a constitutional command and good policy, n349 but the claim is stated unequivocally. Privacy scholars have failed to point out the similarities between this freedom of information theory of the First Amendment and the freedom of contract theory of due process embodied in the Lochner line of cases. n350 This is somewhat surprising given the striking parallels between the traditional understanding of Lochnerism and the First Amendment critique.

The traditional view of Lochner goes something like this: Technological advances inherent in the industrialization of America around the turn of the last century created a series of serious social and economic dislocations, such as unsafe working conditions, unfairly low wages, child labor, sweatshops, and monopolistic trade practices. Reformers including Populists and Progressives sought to remedy these problems of poor working conditions and unequal bargaining power by enacting social legislation. n351 Unfortunately, Supreme Court Justices interpreted the word "liberty" in the Due Process Clauses to mean "freedom of contract," an inalienable right possessed by both workers and employers to buy and sell their labor in a marketplace unfettered by government controls. In so doing, the judges illegitimately read their own pro-business laissez-faire views of political economy into the Due Process Clauses. This interpretation of ""liberty of contract,' the story continues, erected a constitutional barrier to most early twentieth century state or federal legislation directed at hours, wages, and working conditions." n352 However, less activist judges in the mid-twentieth century consigned Lochner to the doctrinal scrapheap, and today Lochner is one of the worst charges that can be leveled against a doctrine or constitutional interpretation, an unequivocal normative repudiation of "courts that appear to be substituting their own view of desirable social policy for that of elected officials." n353

From this perspective, there are some fairly strong parallels between the traditional conception of Lochner and the First Amendment critique of data **[*1213]** privacy legislation. Both theories are jurisprudential responses to calls for legal regulation of the economic and social dislocations caused by rapid technological change. Lochnerism addressed a major socio-technological problem of the industrial age - the power differential between individuals and businesses in newly industrial working conditions - while the First Amendment critique addresses a major socio-technological problem of our information age - the power differential between individuals and businesses over information in the newly electronic environment. Both theories place a libertarian gloss upon the Constitution, interpreting it to mandate either "freedom of contract" or "freedom of information." Both theories seek to place certain forms of economic regulation beyond the power of legislatures to enact. And both theories are eagerly supported by business interests keen to immunize themselves from regulation under the aegis of constitutional doctrine. n354 To the extent that the First Amendment critique is similar to the traditional view of Lochner, then, its elevation of an economic right to first-order constitutional magnitude seems similarly dubious.

Although it might be both tempting and rhetorically effective to accuse the critics of Lochnerism and move on, in the interests of fairness and intellectual honesty it is important to admit that the conventional view of Lochner is probably quite erroneous, at least as a description of the jurisprudence in its actual operation. Legal historians examining the intellectual history of the late nineteenth and early twentieth centuries have significantly revised our understanding of not just Lochner, but also the orthodox legal epistemology that produced it and the ways in which that jurisprudential worldview evolved into the radically different vision of the Constitution, and ultimately law itself, that animates orthodox modern legal thought. n355 Scholarship by these so-called "Lochner revisionists" has significantly revised our understanding of the intellectual contexts in which the cases were decided. Specifically, these scholars have uncovered and made great strides towards reconstructing a coherent vision of law that constituted jurisprudential orthodoxy during the late nineteenth and early twentieth centuries. Termed variously "legal orthodoxy," **[*1214]** "classical legal thought," or "legal formalism," n356 this jurisprudential worldview was an interlocking system of doctrines n357 that represented a functioning classical intellectual engine not unlike the estates system in land law. Formalist legal theory posited that the Constitution had a fixed, essentialist, immanent meaning; that judges could uncover this meaning through ordinary common law modes of inquiry; and that such a mode of inquiry resulted in the judge applying an existing, determined law to new circumstances. n358 Most fundamentally, legal formalism drew a sharp separation between the sources of law and the judges who interpreted those sources; unlike the legal realists,

whose view of law ultimately triumphed over formalism over the course of the first four decades of the twentieth century, formalist judges believed that they discovered law but did not make it. n359

Revisionist scholarship has described the formalist judges as engaging in "guardian review" in constitutional cases, glossing constitutional text with meaning derived from external sources in order to mark out the boundaries between public authority such as the police power and private rights like the liberty protected by the Due Process Clauses. Guardian review was quite different from the modern regime of bifurcated review, according to which courts do not believe that they divine law from external sources, but rather believe that they create it in many instances. Mindful of their countermajoritarian role under an epistemology in which they create rather than divine law, modern courts applying bifurcated review generally treat legislative enactments regarding economic policy with deference, and closely scrutinize only those enactments that interfere with political rights and thus threaten the operation of ordinary democratic processes. n360 In the context of the Due Process Clauses at issue in the Lochner line of cases, the revisionists have demonstrated persuasively that these cases were not merely injections of reactionary pro-business politics into the constitutional text, but were rather interpretations of the Constitution that were consistent with legitimate authority. Such decisions are, the revisionists argue, best explained as determined by settled existing doctrine rather than judges behaving as political actors. n361 Thus, as a descriptive explanation of Lochner, the behavioralist theory of "laissez-faire constitutionalism" is unpersuasive. n362

[*1215] Nevertheless, even in light of the tremendously valuable insights provided by the Lochner revisionists, the First Amendment critique retains enough similarities to the traditional view of Lochner to be normatively questioned from a modern perspective as a jurisprudentially sound application of the First Amendment. Even if Lochner was not an illegitimate injection of pro-business libertarian ideology into constitutional decisionmaking by judges, it was widely condemned as such. Such critiques were made both by contemporaries who accused judges of importing their policy preferences and class biases into their decisions, and by later judges and scholars who replaced guardian review with bifurcated review, in part in reaction to the perceived illegitimacy of Lochner. n363 Thus, merely because the Lochner line of cases appears to have been legitimate under existing doctrine as a descriptive matter, it does not follow as a normative matter that judges should nevertheless be free to inject their view of good social and economic policy into constitutional interpretation. The realists may have been wrong that "liberty of contract" was an empty vessel into which the policy preferences of conservative judges were poured, but this does not mean that judges today can legitimately pour ideological content into the Constitution to void the economic policy of elected representatives. To the extent that the First Amendment critique suggests judges should do something similar in the database context by treating the First Amendment as embodying a "freedom of information" rationale, such an assertion would be similarly illegitimate. In this regard, the modern normative commitment against placing social and economic problems beyond the reach of democratic regulatory politics would still counsel against taking the First Amendment critique at face value.

Alternatively, for a couple of other reasons, one could accept the insights of the Lochner revisionists and still decide quite rationally that Lochnerism (and thus the First Amendment critique) is as illegitimate as the conventional view would suggest. First, as William Wiecek has argued, legal formalism presented a worldview that was attractive to lawyers because it protected wealth and placed the regulation of property rights beyond the power of legislatures to redistribute. n364 Thus, the reconstruction of the doctrinal coherence of Lochner would not displace the suggestion that lawyers could find formalist jurisprudence attractive as a purely instrumental matter because it produced outcomes they favored. To the contrary, it would merely confirm **[*1216]** that the elite lawyers who subscribed to and articulated Lochnerism were merely good advocates who had thought through the intellectual clarity of their position. It would not, however, say anything about the merits of that position other than its intellectual elegance.

Second, even if Lochner were legitimate under established doctrine, it could nevertheless be illegitimate for other reasons. Barry Friedman has argued that even though the Lochner line of cases was consistent with formalist doctrine, the jurisprudence was widely criticized as illegitimate by the larger public. n365 Like Wiecek's lawyers, who found Lochner attractive because of its outcomes, progressive critics also repudiated it because it created outcomes they found unjust. In this context, Barry Friedman draws a distinction between "legal legitimacy" - whether legal decisions have "an established jurisprudential basis" - and what he calls "social legitimacy" - an inquiry that "looks beyond

jurisprudential antecedents of constitutional decisions and asks whether those decisions are widely understood to be the correct ones given the social and economic milieu in which they are rendered." n366 Friedman points to the widespread contemporary popular disagreement with the outcomes of liberty of contract cases as an example of such illegitimacy. n367 And in the modern context, the enormous public outcry and prompt congressional action surrounding the judicial invalidation of the FCC's Do-Not-Call Registry similarly suggests that there is little tolerance today for constitutionalizing information policy. n368

The parallels between the First Amendment critique and the traditional view of Lochner are not perfect, but they should at least serve to caution us against an uncritical acceptance of the First Amendment critique. The database problem represents a particularly thorny instance of a social problem created by rapid advances in technology. Just as no simple regulatory solution is likely to produce an optimal result, so too is no simple constitutional solution likely to do the same. Because both coverage of the First Amendment and its doctrine are unclear, facile constitutional mantras like "freedom of information" are particularly ill-suited to resolve a complex problem in a means **[*1217]** that is satisfactory to society as a whole. As I have argued above, it would be a great tragedy for the continued ascendance of the First Amendment critique to handicap or prohibit elected policymakers from exploring such a difficult question of social and economic policy. n369

B. The First Amendment Critique and the Bifurcated Review Project

If the jurisprudential problems caused by the First Amendment critique seem significant from the perspective of privacy law, they are even more dire from the perspective of First Amendment law. Indeed, the same intellectual history of rights jurisprudence that complicates the traditionalist view of Lochner brings the real jurisprudential threat of the First Amendment critique into sharp focus. At stake in the database debate is not merely whether data privacy rules can be enforced consistent with the First Amendment, but rather what sorts of rights the First Amendment protects at all. At bottom, the First Amendment critique proffers a robust rationale of freedom of information that threatens the very structure of modern rights jurisprudence - the bifurcated system of judicial review that defers to legislatures with respect to economic rights but treats laws infringing upon political rights with greater scrutiny.

Modern legal historians have devoted significant attention to the task of reconstructing the jurisprudential universe of legal formalism that produced Lochnerian rights jurisprudence, but they have spent far less time examining the ways in which the Supreme Court laid the foundations for the rights jurisprudence that replaced it. n370 As I have suggested elsewhere, much of this work was done by the Court in a series of cases that roughly corresponded with the Second World War, many of which involved free speech and free exercise challenges brought by the Jehovah's Witnesses. n371 Only a handful of modern scholars have devoted much serious effort to reconstructing this critical episode in the intellectual history of American law, but the work they have done sheds significant light on the origins of modern rights jurisprudence.

This revisionist rights scholarship has shown how the Supreme Court used the First Amendment as a bridge between the old regime of guardian review and the modern regime of bifurcated review. n372 The Court outlined this new approach in "famous footnote four" of the 1938 case of United States v. **[*1218]** Carolene Products Co., n373 which posited a relaxed standard of review for economic regulation but a more stringent standard of review for laws that infringed upon rights guaranteed by the text of the Bill of Rights or otherwise interfered with the democratic process. n374 As G.E. White explains, this system of "bifurcated review" embodied two of the central assumptions of the new jurisprudence:

By fostering judicial deference in the area of economic regulation, the project embraced the perceived truth that unregulated economic activity actually infringed on the freedom of a significant number of actors in the economic marketplace and reinforced rational regulatory policies that were based on that truth. By fostering judicial scrutiny of legislative restrictions on speech and other noneconomic liberties, the project underscored the centrality of the

modernist freedom premise when that premise could be associated with the goals of democratic theory. n375

Central to the dualism at the core of the new system of judicial review was a strict separation between economic and political rights. Thus, as noted above, n376 the Supreme Court initially excluded commercial speech from heightened First Amendment protection in Valentine v. Chrestensen n377 and Breard v. Alexandria, n378 in order to maintain this separation. In another case involving the distribution of literature, Justice Douglas drew a sharp distinction between religious texts covered by "the privileges protected by the First Amendment" and advertising, which he dismissed as "the wares and merchandise of hucksters and peddlers." n379

The sharp line between economic and political rights critical to the intellectual coherence of bifurcated review has persisted, though it perhaps has not endured with the precise clarity that its drafters intended. Indeed, it is in the advertising cases that the greatest blurring of the line between political and economic rights has occurred. After a series of cases indicating that certain forms of advertising associated (quite ironically) with the privacy rights protected in Griswold and Roe warranted heightened protection, the Court in Virginia State Board of Pharmacy v. Virginia Citizens Consumer Council, Inc. n380 brought "commercial speech" within the scope of the First Amendment. In drafting the opinion of the Court, Justice Blackmun was confronted with **[*1219]** the conceptual problem that as an economic right, the right to advertise was not supported by any of the existing justifications for free speech. He solved this problem by making one up:

As to the particular consumer's interest in the free flow of commercial information, that interest may be as keen, if not keener by far, than his interest in the day's most urgent political debate... . Generalizing, society also may have a strong interest in the free flow of commercial information. Even an individual advertisement, though entirely "commercial," may be of general public interest. n381

Blackmun went on to add:

Advertising, however tasteless and excessive it sometimes may seem, is nonetheless dissemination of information as to who is producing and selling what product, for what reason, and at what price. So long as we preserve a predominantly free enterprise economy, the allocation of our resources in large measure will be made through numerous private economic decisions. It is a matter of public interest that those decisions, in the aggregate, be intelligent and well informed. To this end, the free flow of commercial information is indispensable. n382

Taken at face value, Blackmun's rationale for heightened constitutional protection for commercial advertising threatened to dissolve the line between economic and political speech - and with it any distinction between economic and political rights. In so doing, he opened the door to the resuscitation of Lochner-style economic rights (or at least the traditional understanding of those rights). This fact was not lost on a few contemporary observers, be they dissenting members of the Court n383 or scholarly commentators. n384 Indeed, in the aftermath of the decision, observers predicted the expansion of First **[*1220]** Amendment analysis to other areas of business speech regulation like securities law. n385 However, the fears raised by these commentators failed to materialize.

The line between economic and political rights has persisted, and it remains central to the continued coherence of the modern system of bifurcated review. An expansive reading of Virginia Pharmacy as opening the floodgates to heightened review for other economic speech rights besides advertising was rejected, and the dividing line between economic and political rights was shored up in its new location, with commercial advertising placed upon the political rights side of the line. Thus, the feared treatment of securities speech as commercial speech did not come to pass, and the large categories of speech that fall outside the scope of the First Amendment have not been subjected to heightened constitutional review. n386 Although the balance is a delicate one, nonadvertising speech in the commercial context

continues to be assessed properly under the rational basis review afforded to the other economic rights by the bifurcated review project. n387

Looking at the issue from the perspective of free speech law allows a better appreciation of the threat to the modern scheme of rights jurisprudence represented by the First Amendment critique. The critics' attempt to clothe economic rights with the garb of political rights would destroy the basic dualism on which the edifice of modern rights jurisprudence is built. This may not be their intent, but it would be the likely effect of their success. In the database context, this might mean only that nondisclosure rules are treated with heightened scrutiny, but the advancement of a principle of freedom of information as a full-blooded rationale for heightened First Amendment scrutiny would not be limited merely to that context. Every regulation that could be classified as restricting "speech" or information flows would be brought within the scope of First Amendment heightened review. Indeed, much of Volokh's own First Amendment scholarship, in addition to his influential privacy article, has tracked such a prediction, subjecting previously nonsalient areas of speech regulation to more searching doctrinal analysis. n388

[*1221] A reasonable person could certainly argue that the First Amendment should apply to everything that the dictionary might deem to be "speech." It might also be reasonable to argue that information flows generally should be treated to heightened constitutional protection, although this would complicate regulation of not only the database problem but also the entire information economy, with spillover effects into areas such as intellectual property. n389 It might even be reasonable to argue that the distinction between political and economic rights is unwise, unworkable, or even illegitimate, as some prominent scholars have recently asserted. n390 However, such a system would not be our system, and it would likely mean the end of bifurcated review's distinction between political and economic rights. If we are to make such a change legitimately and coherently, it should come overtly, not by allowing the Virginia Pharmacy rationale of freedom of information gradually to undermine the distinction between political and economic rights.

Conclusion

Over four decades ago, before the advent of the Internet or the introduction of freedom of information as a theoretical justification for the First Amendment, Thomas Emerson examined the intersection of privacy and the First Amendment. Emerson noted:

Any society sincerely interested in protecting the right of privacy is hardly likely to be at the same time hostile to the right of free expression. Both interests tend to have the same friends and the same enemies. The chief danger is that the right of privacy will be used as a screen, by those not really interested in either interest, to infringe upon legitimate expression. This danger can be met if the courts actively insist upon a careful definition of a genuine right of privacy and upon a fair accommodation of the two interests. n391 **[*1222]** Emerson had in mind the same paradigmatic privacy case as his contemporary Prosser - the case against a newspaper for publishing private facts. n392 However, the data privacy cases envisioned by the First Amendment critics are in some respects the mirror image of what Emerson describes. In these cases, the First Amendment is being used as the screen, to infringe upon legitimate modes of government privacy regulation.

This Article has attempted to follow Emerson's advice in the modern context, arguing that when we subject both data privacy regulations and the First Amendment to careful scrutiny, they can be reconciled without sacrificing either. Furthermore, the real danger presented by the tension between privacy and the First Amendment is not that we must choose one over the other, but that we must instead avoid constitutionalizing important public law issues. Lurking behind the facade of seemingly neutral arguments by First Amendment critics is a theory of free speech and rights jurisprudence more generally that has the potential to topple the edifice of modern constitutionalism. If we do not reject such a theory, we may lose both our "genuine right of privacy" and our system of bifurcated review, under which civil and political rights are protected from legislatures, but economic rights generally are determined by the political process.

At the level of policy, however, resolving the conceptual problem does little to reduce the complexity of the

database problem. Indeed, looking at the constitutional issues in the way I propose only allows policymakers to face the true challenges of the database problem and the regulation of information flows. Such a challenge likely will be as thorny in the information age as the problem of regulating industrial capitalism has been for over a century. And there are likely to be no easy answers to this new problem. In fact, in many instances freedom of information may well be the best policy; in others, privacy regulation may produce unacceptable social costs or be technically infeasible. Indeed, we may well determine that more privacy regulations are a really bad idea. However, this calculus should be made at the level of policy rather than at the abstract level of constitutional theory. Anything else would be inconsistent with the basic premises upon which modern rights jurisprudence rests.

Legal Topics:

For related research and practice materials, see the following legal topics:
Constitutional LawBill of RightsFundamental FreedomsFreedom of SpeechCommercial SpeechGeneral OverviewConstitutional LawBill of RightsFundamental FreedomsFreedom of SpeechExpressive ConductConstitutional LawBill of RightsFundamental FreedomsFreedom of SpeechScope of Freedom

FOOTNOTES:

n1. See, e.g., Fred H. Cate, Privacy in the Information Age (1997); Lawrence Lessig, Code and Other Laws of Cyberspace (1999); Daniel J. Solove, The Digital Person: Technology and Privacy in the Information Age (2004); Technology and Privacy: The New Landscape (Philip E. Agre & Marc Rotenberg eds., 1997); Stan Karas, Privacy, Identity, Databases, 52 Am. U. L. Rev. 393 (2002); Daniel J. Solove, Privacy and Power: Computer Databases and Metaphors for Information Privacy, 53 Stan. L. Rev. 1393 (2001).

n2. Scholars grappling with the "database problem" have argued that the rights of individuals are threatened by detailed private-sector databases containing profiles of their preferences. These profiles contain potentially embarrassing information, including information about their health, political views, or sexual activities or inclinations. See generally Solove, supra note 1, at 13-26.

n3. Eugene Volokh, Freedom of Speech and Information Privacy: The Troubling Implications of a Right to Stop People From Speaking About You, 52 Stan. L. Rev. 1049, 1051 (2000).

n4. Samuel D. Warren & Louis D. Brandeis, The Right to Privacy, 4 Harv. L. Rev. 193 (1890); see also Lawrence M. Friedman, American Law in the Twentieth Century 369 (2002); Dorothy J. Glancy, The Invention of the Right to Privacy, 21 Ariz. L. Rev. 1, 1 (1979); Diane L. Zimmerman, Requiem for a Heavyweight: A Farewell to Warren and Brandeis's Privacy Tort, 68 Cornell L. Rev. 291, 292 (1983).

N5. See Warren & Brandeis, supra note 4, at 195.

n6. See, e.g., Glancy, supra note 4, at 1; Zimmerman, supra note 4, at 292.

n7. 274 U.S. 357, 372-80 (1927) (Brandeis, J., concurring).

n8. See Harry Kalven, Jr., A Worthy Tradition: Freedom of Speech in America 156-66 (1988); David M. Rabban, Free Speech in Its Forgotten Years 369 (1997); G. Edward White, The Constitution and the New Deal 143 (2000); Ashutosh A. Bhagwat, The Story of Whitney v. California: The Power of Ideas, in Constitutional Law Stories 407, 407-08 (Michael C. Dorf ed., 2004); Vincent Blasi, The First Amendment and the Ideal of Civic Courage: The Brandeis Opinion in Whitney v. California, 29 Wm. & Mary L. Rev. 653, 668 (1988).

n9. See Kent Gormley, One Hundred Years of Privacy, 1992 Wis. L. Rev. 1335.

n10. See Jerry Kang, Information Privacy in Cyberspace Transactions, 50 Stan. L. Rev. 1193, 1202 (1998); Daniel J. Solove, Conceptualizing Privacy, 90 Cal. L. Rev. 1087, 1088 (2002).

n11. See infra Part II.

n12. See, e.g., Bartnicki v. Vopper, 532 U.S. 514 (2001).

n13. N.Y. Times Co. v. Sullivan, 376 U.S. 254, 270 (1964).

n14. See infra note 71 and accompanying text.

n15. For a detailed discussion of the database problem, see sources cited supra note 1.

n16. See, e.g., Robert Ellis Smith, Ben Franklin's Web Site: Privacy and Curiosity From Plymouth Rock to the Internet 12 (2000); David Banisar & Simon Davies, Global Trends in Privacy Protection: An International Survey of Privacy, Data Protection, and Surveillance Laws and Developments, 18 J. Marshall J. Computer & Info. L. 1, 31-32 (1999); Solove, supra note 1, at 1400 & n.29.

n17. See Act of Mar. 1, 1889, ch. 319, 8, 13, 25 Stat. 760 (imposing $ 500 fine for disclosure of census information); see also Note, The Right to Privacy in Nineteenth Century America, 94 Harv. L. Rev. 1892, 1905 (1981).

n18. See Ballard C. Campbell, The Growth of American Government 231-32 (1995).

n19. See id. at 232.

n20. United States Dep't of Justice v. Reporters Comm. for Freedom of the Press, 489 U.S. 749, 770 (1989) (quoting Whalen v. Roe, 429 U.S. 589, 605 (1977)).

n21. See Daniel J. Solove, Access and Aggregation: Public Records, Privacy, and the Constitution, 86 Minn. L. Rev. 1137, 1138 (2002).

n22. For example, the Privacy Act of 1974, 5 U.S.C. 552a (2000), gives individuals certain rights with respect to data about them in federal government databases.

n23. E.g., Nixon v. Adm'r of Gen. Servs., 433 U.S. 425 (1977); Whalen, 429 U.S. 589. Backstopping this constitutional protection is the Freedom of Information Act, 5 U.S.C. 552. Although the Act generally provides for public access to information held by the government, it exempts from disclosure certain categories of government information, the disclosure of which might constitute an "unwarranted invasion of personal privacy." Id. 552(b)(6), 552(b)(7)(C).

n24. See, e.g., Solove, supra note 1, at 19; Philip E. Agre, Introduction to Technology and Privacy: The New Landscape, supra note 1, at 1, 3; Elec. Privacy Info. Ctr., Privacy and Consumer Profiling, at http://www.epic.org/privacy/profiling/.

n25. See Solove, supra note 1, at 1404.

n26. Such companies are also known as "commercial data brokers," or "CDBs." See generally Chris J. Hoofnagle, Big Brother's Little Helpers: How ChoicePoint and Other Commercial Data Brokers Collect and Package Your Data for Law Enforcement, 29 N.C. J. Int'l L. & Com. Reg. 595 (2004).

n27. Elec. Privacy Info. Ctr., supra note 24.

n28. See id.

n29. See A. Michael Froomkin, The Death of Privacy?, 52 Stan. L. Rev. 1461, 1473-74 (2000); see also Solove, supra note 1, at 18-21 (collecting other examples).

n30. See Ely R. Levy & Norman I. Silber, Nonprofit Fundraising and Consumer Protection: A Donor's Right to Privacy, 15 Stan. L. & Pol'y Rev. 519, 543-44 (2004).

n31. See, e.g., Karas, supra note 1, at 437-39.

n32. See, e.g., John Rothchild, Protecting the Digital Consumer: The Limits of Cyberspace Utopianism, 74 Ind. L.J. 893, 972-73 (1999).

n33. See Daniel J. Solove, Identity Theft, Privacy and the Architecture of Vulnerability, 54 Hastings L.J. 1227 (2003).

n34. One of the most alarming incidents involves the case of Amy Boyer, who was murdered at her workplace by a man who received Boyer's date of birth, social security number, home address, and work address

from an information broker. The information broker had used pretexting - using already available information and lying about one's identity and purpose - to get Boyer to reveal her employment information. See Remsburg v. Docusearch, Inc., 816 A.2d 1001, 1009 (N.H. 2003).

n35. In one case, a major profiling company used inmates to process consumer data surveys. One of the prisoners used information from one woman's survey - including her name, address, buying habits, and medical information - to harass her, sending her a sexually explicit letter sprinkled with personal, identifying details and proposing to visit her home upon his release. See Stanley S. Arkin, Misuse and Misappropriation of Electronically Stored Information, N.Y. L.J., July 23, 2001, at 3.

n36. Perhaps the most sinister such use of business records occurred in 1940, when the invading German armies used business records, among other sources, to identify Jews for roundup by the Gestapo. See Richard Sobel, The Degradation of Political Identity Under a National Identification System, 8 B.U. J. Sci. & Tech. L. 37, 52 (2002); see also Wayne Madsen, Handbook of Personal Data Protection 22-23 (1992).

n37. See Hoofnagle, supra note 26, at 611 (noting that database companies package personal data for sale to law enforcement and offer substantial discounts to government customers).

n38. See Robert O'Harrow, Jr., In Terror War, Privacy vs. Security, Wash. Post, June 3, 2002, at A1; see also Karen E. Jones, Comment, The Effect of the Homeland Security Act on Online Privacy and the Freedom of Information Act, 72 U. Cin. L. Rev. 787 (2003).

n39. See Solove, supra note 1, at 168-74.

n40. See Hoofnagle, supra note 26, at 635-37.

n41. For varying estimates, see Ted Bridis, Industry Studies Attack Web-Privacy Laws, Wall St. J., Mar. 13, 2001, at B6 (estimating that regulation would cost the ninety largest financial institutions $ 17 billion per year); see also Robert W. Hahn, An Assessment of the Costs of Proposed Online Privacy Legislation 22-23 & tbl.2 (2001) (estimating a $ 36 billion cost for online privacy regulation), available at http://www.bbbonline.org/UnderstandingPrivacy/library/whitepapers/hahnstudy.pdf; Kent Walker, The Costs of Privacy, 25 Harv. J.L. & Pub. Pol'y 87 (2001) (estimating a $ 17.6 billion cost of privacy legislation relating to medical information costs).

n42. Walker, supra note 41, at 87-88.

n43. Robert W. Hahn & Anne Layne-Farrar, The Benefits and Costs of Online Privacy Legislation, 54 Admin. L. Rev. 85, 158-61 (2002).

n44. See, e.g., Richard A. Posner, Overcoming Law 531-51 (1995); Richard A. Posner, Blackmail, Privacy, and Freedom of Contract, 141 U. Pa. L. Rev. 1817 (1993); Richard A. Posner, The Right of Privacy, 12 Ga. L. Rev. 393 (1978); George J. Stigler, An Introduction to Privacy in Economics and Politics, 9 J. Legal Stud. 623, 632-33 (1980). But see Richard S. Murphy, Property Rights in Personal Information: An Economic Defense of Privacy, 84 Geo. L.J. 2381, 2397-99 (1996) (arguing that privacy rules are rational from a law and economics perspective).

n45. See, e.g., Fred H. Cate, First Amendment Ctr., The Privacy Problem: A Broader View of Information Privacy and the Costs and Consequences of Protecting It (2003), available at http://www.firstamendmentcenter.org/PDF/FirstReport.privacyproblem.pdf; Hahn, supra note 41; Paul H. Rubin & Thomas M. Lenard, Privacy and the Commercial Use of Personal Information 8-9 (2002); Kent Walker, Where Everybody Knows Your Name: A Pragmatic Look at the Costs of Privacy and the Benefits of Information Exchange, 2000 Stan. Tech. L. Rev. 2, P 21-33, at http://stlr.stanford.edu/STLR/Articles/00_STLR_2/index.htm; see also Fed. Trade Comm'n, Privacy Online: Fair Information Practices in the Electronic Marketplace (2000) (dissenting statement of Commissioner Orson Swindle), available at http://www.ftc.gov/os/2000/05/privacyswindle.htm.

n46. See Hahn & Layne-Farrar, supra note 43 (collecting and assessing numerous such proposals).

n47. See, e.g., Julie E. Cohen, Examined Lives: Informational Privacy and the Subject as Object, 52 Stan. L. Rev. 1373, 1375-76 (2000).

n48. See infra note 71.

n49. Volokh, supra note 3, at 1050-51.

n50. Id. at 1051.

n51. Id. at 1122.

n52. Id. at 1051; see also id. at 1051 & n.4, 1116 (stating that "Codes of fair information practices" to protect privacy rights would not only "raise[] serious First Amendment problems" but would also make it "much easier for people to accept "codes of fair reporting,' "codes of fair debate,' "codes of fair filmmaking,' "codes of fair political criticism,' and the like." (footnote omitted)). Volokh expands on the issue of slippery slopes at a more general level in Eugene Volokh, The Mechanisms of the Slippery Slope, 116 Harv. L. Rev. 1026 (2003).

n53. See Cate, supra note 1, at 68-71. Cate concludes that "any government effort to protect privacy, either directly or through the passage or enforcement of laws permitting suits by private parties, faces significant First Amendment obstacles." Id. at 71; see also Cate, supra note 45, at 10-22; Fred H. Cate, The First Amendment and the National Information Infrastructure, 30 Wake Forest L. Rev. 1, 48-50 (1995); Fred H. Cate & Robert Litan, Constitutional Issues in Information Privacy, 9 Mich. Telecomm. & Tech. L. Rev. 35, 49-58 (2002).

n54. Solveig Singleton, Privacy Versus the First Amendment: A Skeptical Approach, 11 Fordham Intell. Prop. Media & Ent. L.J. 97, 132-53 (2000).

n55. Solveig Singleton, Privacy as Censorship: A Skeptical View of Proposals to Regulate Privacy in the Private Sector (Cato Inst. Policy Analysis No. 295, 1998), at http://www.cato.org/pubs/pas/pa-295.html; Solveig Singleton, Reviving a First Amendment Absolutism for the Internet, 3 Tex. Rev. L. & Pol. 279 (1999) (arguing more generally for stronger First Amendment protection in the electronic context).

n56. In addition to Volokh, supra note 3, and Solveig Singleton's articles, supra notes 54-55, see, for example, Tom W. Bell, Internet Privacy and Self-Regulation: Lessons From the Porn Wars 6-7 (Cato Inst., 2001), available at http://www.cato.org/pubs/briefs/bp65.pdf; Jeremy D. Mishkin, Media Law Resource Ctr., Privacy Online 2.0, at 11-13 (2002), at http://www.medialaw.org/Template.cfm?Section=Archive7&Template=/ContentManagement/ContentDisplay.cfm&ContentID=1
Tom W. Bell, Pornography, Privacy, and Digital Self Help, 19 J. Marshall J. Computer & Info. L. 133, 144-46 (2000); Bruce E.H. Johnson, The Battle Over Internet Privacy and the First Amendment, Computer & Internet L., Apr. 2001, at 21; Bruce E.H. Johnson & Kavita Amar, Privacy Questions Arising in the Context of Commercial Speech, in 1 Communications Law 2002, at 7, 7-8 (PLI Intellectual Prop. Practice Course,

Handbook Series No. G-726, 2002); Robert A. Levy, Turn the Ringer Off, Nat'l Rev. Online, Oct. 2, 2003, at http://www.nationalreview.com/comment/levy200310020827.asp (arguing that the FCC's Do-Not-Call Registry violates the First Amendment); Jonathan M. Winer, Regulating the Free Flow of Information: A Privacy Czar as the Ultimate Big Brother, 19 J. Marshall J. Computer & Info. L. 37, 47 & n.47 (2000).

n57. Robert M. O'Neil, The First Amendment and Civil Liability 74-90 (2001).

n58. Rodney A. Smolla, Privacy and the First Amendment Right to Gather News, 67 Geo. Wash. L. Rev. 1097, 1138 (1999) ("As matters stand today, strong First Amendment doctrines stand in the way of many of the most meaningful privacy reforms.").

n59. Froomkin, supra note 29, at 1521-23 (concluding that the First Amendment raises serious questions about the constitutionality of existing federal privacy statutes).

n60. Brief for Appellant at 6, U.S. West, Inc. v. FCC, 182 F.3d 1224 (10th Cir. 1999) (No. 98-3451).

n61. See, e.g., Vera Bergelson, It's Personal, But Is It Mine? Towards Property Rights in Personal Information, 37 U.C. Davis L. Rev. 379, 396-400 (2003) (noting that the First Amendment problems identified by Volokh, Singleton, and others should significantly shape the legal response to consumer privacy issues); Walker, supra note 41, at 123. Walker writes:

Recognizing that we are legislating in the shadow of the First Amendment suggests a powerful guiding principle for framing privacy regulations. Like any laws encroaching on the freedom of information, privacy regulations must be narrowly tailored and powerfully justified... . Legislators should identify a specific and real harm and tailor any responsive laws narrowly.

Id.; see also Stan Karas, Enhancing the Privacy Discourse: Consumer Information Gathering as Surveillance, 7 U. Fla. J. Tech. & Pol'y 3 (2002); James P. Nehf, Incomparability and the Passive Virtues of Ad Hoc Privacy Policy, 76 U. Colo. L. Rev. 1, 26-27 (2005); Peter A. Winn, Confidentiality in Cyberspace: The HIPAA Privacy Rules and the Common Law, 33 Rutgers L.J. 617, 675 (2002); William McGeveran, Note, Programmed Privacy Promises: P3P and Web Privacy Law, 76 N.Y.U. L. Rev. 1812, 1822-24 (2001) (arguing that First Amendment principles render many consumer privacy rules unconstitutional, and shape outcomes); Scott Shorr, Note, Personal Information Contracts: How to Protect Privacy Without Violating the First Amendment, 80 Cornell L. Rev. 1756, 1811-18 (1995) (proposing a contractual approach to the problem of consumer credit reports because credit companies have a First Amendment right to disclose consumer credit information); Kyle Thomas Sammin, Note, Any Port in a Storm: The Safe Harbor, The Gramm-Leach-Bliley Act, and the Problem of

Privacy in Financial Services, 36 Geo. Wash. Int'l L. Rev. 653, 656 (2004).

n62. 182 F.3d 1224.

n63. 16 C.F.R. 310.4(b)(1)(iii)(B) (2004).

n64. Mainstream Mktg. Servs. Inc. v. FTC, 283 F. Supp. 2d 1151, 1167-68 (D. Colo. 2003), rev'd, 358 F.3d 1228, 1241 (10th Cir. 2004).

n65. I have argued elsewhere that the Tenth Circuit's reversal of the lower court was correct, both as a doctrinal and a normative matter. See Caroline E. Mayer, National No-Call List Upheld by Court, Wash. Post, Feb. 18, 2004, at E1 (""The court [correctly] concluded that the right of people to enjoy their homes outweighs the right of companies to intrude upon that privacy to try and sell them things,' Richards said.").

n66. Mainstream Mktg. Servs., 358 F.3d at 1250-51.

n67. See, e.g., L.A. Police Dep't v. United Reporting Publ'g Corp., 528 U.S. 32 (1999); United Reporting Publ'g Corp. v. Cal. Highway Patrol, 146 F.3d 1133, 1140 (9th Cir. 1998) (holding a California statute prohibiting release of arrestee names and addresses for commercial purposes unconstitutional under the Central Hudson test). In the context of credit report regulation, other courts have accepted the critique's premise that the sale of databases is "speech," but these courts have applied intermediate scrutiny and found the privacy interests sufficient to outweigh the business speech interests. See, e.g., Trans Union Corp. v. FTC, 245 F.3d 809, 818-19 (D.C. Cir. 2001) (restricting a consumer reporting agency's sale of targeted marketing lists did not violate the First Amendment); Individual Reference Servs. Corp. v. FTC, 145 F. Supp. 2d 6 (D.D.C. 2001), aff'd sub nom. Trans Union LLC v. FTC, 295 F.3d 42 (D.C. Cir. 2002). But see Equifax Servs., Inc. v. Cohen, 420 A.2d 189 (Me. 1980) (invalidating under the First Amendment a state law requiring the consent of a consumer before a firm could request that consumer's credit history).

n68. See, e.g., Trans Union LLC v. FTC, 536 U.S. 915 (2002) (Kennedy, J., dissenting from denial of certiorari).

n69. See Johnson, supra note 56, at 23-24.

n70. See, e.g., Thomas I. Emerson, Toward a General Theory of the First Amendment 76 (1966) ("Any society sincerely interested in protecting the right of privacy is hardly likely to be at the same time hostile to the right of free expression. Both interests tend to have the same friends and the same enemies.").

n71. The only piece that challenges the critique in depth is Daniel J. Solove, The Virtues of Knowing Less: Justifying Privacy Protections Against Disclosure, 53 Duke L.J. 967 (2003). Solove's concern, however, is to justify privacy nondisclosure rules more generally (that is, outside the database context), not only against a First Amendment critique, but also against other normative challenges to keeping information private. Id. at 969-76. As I explain infra Part II, my approach to the First Amendment diverges significantly from Solove's, as I believe he grants too much ground to the First Amendment critics. Other scholars who have addressed the First Amendment critique of data privacy in a more abbreviated fashion include Cohen, supra note 47, at 1409-23, providing a thoughtful theoretical overview of data privacy issues and devoting fourteen pages to the issue; Kang, supra note 10, at 1287, providing a proposal for online privacy reform; and Paul Schwartz, Free Speech vs. Information Privacy: Eugene Volokh's First Amendment Jurisprudence, 52 Stan. L. Rev. 1559 (2000), a symposium comment to Volokh's article.

n72. See infra Part IV.

n73. Volokh, supra note 3, at 1050-51 (citations omitted).

n74. See Schwartz, supra note 71, at 1561.

n75. See Marc Rotenberg, Fair Information Practices and the Architecture of Privacy (What Larry Doesn't Get), 2001 Stan. Tech. L. Rev. 1, P 8, at http://stlr.stanford.edu/STLR/Articles/01_STLR_1/index.htm.

n76. U.S. Dep't of Health, Educ. & Welfare, Records, Computers, and the Rights of Citizens: Report of the Secretary's Advisory Comm. on Automated Personal Data Systems (1973), available at http://www.epic.org/privacy/hew1973report/.

n77. 5 U.S.C. 552a (2000).

n78. For an assessment of the Privacy Act, see Robert Gellman, Does Privacy Law Work?, in Technology and Privacy: The New Landscape, supra note 1, at 193.

n79. See Schwartz, supra note 71, at 1561 n.12; see also Paul M. Schwartz & Joel R. Reidenberg, Data Privacy Law 5 (1996).

n80. See Gellman, supra note 78, at 196.

n81. Joel R. Reidenberg, Setting Standards for Fair Information Practice in the U.S. Private Sector, 80 Iowa L. Rev. 497, 514-15 (1995). For an alternate but equivalent formulation of these principles, see Gellman, supra note 78, at 195-202.

n82. For a comprehensive overview of the many federal statutes governing private sector records, see generally Daniel J. Solove & Marc Rotenberg, Information Privacy Law 491-566 (2003).

n83. 15 U.S.C.A. 1681-1681t (West 1998 & Supp. 2004) (regulating the disclosure and the use of consumer credit information, and giving consumers the right to receive copies of credit records and to correct erroneous information contained in such records).

N84. 18 U.S.C.A. 2511 (West 2000 & Supp. 2004) (prohibiting, inter alia, intentional interception of contents of telephone conversations or e-mail, and disclosure of contents of such communications to others).

n85. 18 U.S.C. 2710 (2000) (prohibiting video stores from disclosing to third parties videos that its customers have rented). The great irony of the VPPA is that it was passed in reaction to the disclosure of Supreme Court nominee Robert Bork's video records during his confirmation. Bork's nomination was defeated in part because of his opposition to a constitutional right of privacy. See Richard C. Turkington & Anita L. Allen, Privacy Law 494 (2d ed. 2002).

n86. 20 U.S.C.A. 1232g (West 2000 & Supp. 2004) (regulating the disclosure of educational records maintained by primary, secondary, and postsecondary institutions that receive federal funds).

n87. See, e.g., 18 U.S.C.A. 2511(4)(a) (criminally punishing violations with fines up to $ 10,000 and up to five years imprisonment); Id. 2520(b)-(c) (authorizing a civil action for violations under which successful plaintiffs can obtain, in addition to attorney's fees and punitive damages, compensatory damages equal to the greater of (1) the sum of actual damages and defendant's profit as a result of the violation or (2) statutory damages equal to the greater of $ 100 per day of violation or $ 10,000).

n88. Schwartz, supra note 71, at 1561-62.

n89. Id. at 1562.

n90. See, e.g., Volokh, supra note 3, at 1054-55.

n91. Id. at 1049.

n92. See infra Part III.

n93. See infra Part IV.

n94. See Schwartz, supra note 71, at 1564; Solove, supra note 71, at 975-1032 (considering and rejecting this approach); Volokh, supra note 3, at 1080-87 (same). One notable exception is Julie Cohen, who has suggested at a theoretical level that regulation of information markets might not implicate heightened First Amendment review. Cohen, supra note 47, at 1417. Cohen's arguments are thoughtful, although she does not develop them in detail and notes that "much work remains to be done." Id. at 1415-16. Nevertheless, my argument in this part builds undeniably upon Cohen's nuanced and sophisticated analysis.

n95. See, e.g., Frederick Schauer, First Amendment Opportunism, in Eternally Vigilant: Free Speech in the Modern Era 175 (Lee C. Bollinger & Geoffrey R. Stone eds., 2002).

n96. Daniel Farber estimates that "the Supreme Court has decided well over two hundred First Amendment cases, most of them since 1970." Daniel A. Farber, The First Amendment 1-2 (2d ed. 2003).

n97. One leading casebook cites 395 principal First Amendment articles in its table of authorities. Geoffrey R. Stone et al., The First Amendment 633-41 (2d ed. 2003).

n98. Or indeed any issue of the applicability of a constitutional right more generally. See Frederick Schauer, The Boundaries of the First Amendment: A Preliminary Exploration of Constitutional Salience, 117 Harv. L. Rev. 1765, 1771 (2004).

n99. Id. at 1769.

n100. Kent Greenawalt, Speech, Crime, and the Uses of Language 40 (1989).

n101. Harry Kalven, Jr., The Reasonable Man and the First Amendment: Hill, Butz, and Walker, 1967 Sup. Ct. Rev. 267, 278.

n102. See generally C. Edwin Baker, Scope of the First Amendment Freedom of Speech, 25 UCLA L. Rev. 964 (1978); see also Laurent B. Frantz, The First Amendment in the Balance, 71 Yale L.J. 1424, 1434-35 (1962); Martin H. Redish, Killing the First Amendment With Kindness: A Troubled Reaction to Collins and Skover, 68 Tex. L. Rev. 1147, 1149-50 (1990).

n103. Kalven, supra note 101, at 278.

n104. Frantz, supra note 102, at 1436.

n105. Schauer, supra note 98, at 1769. See generally id. at 1769 & nn.10-11 (collecting sources).

n106. Id. at 1769.

n107. Greenawalt, supra note 100, at 58, 79-87; Kent Greenawalt, Criminal Coercion and Freedom of Speech, 78 Nw. U. L. Rev. 1081 (1983); Kent Greenawalt, Speech and Crime, 1980 Am. B. Found. Res. J. 645.

n108. See Greenawalt, supra note 100, at 79-140 (collecting cases).

n109. See U.S. Const. amend. I.

n110. Schauer, supra note 98, at 1777-84.

n111. Id. at 1768.

n112. See Erwin Chemerinsky, Constitutional Law 474, 529-30 (2001).

n113. See id. at 695.

n114. Kovacs v. Cooper, 336 U.S. 77, 97 (1949) (Frankfurter, J., concurring).

n115. Virginia v. Black, 538 U.S. 343 (2003) (holding that state bans on "true threats" are compatible with the First Amendment); see also R.A.V. v. City of St. Paul, 505 U.S. 377, 388 (1992) ("Threats of violence are

outside the First Amendment ... .").

n116. Roth v. United States, 354 U.S. 476, 485 (1957) (holding that obscene materials are outside the scope of First Amendment protection); see also Miller v. California, 413 U.S. 15, 24 (1973) (establishing a three-part test for determining whether speech is obscene and therefore outside First Amendment protection).

n117. N.Y. Times Co. v. Sullivan, 376 U.S. 254, 268 (1964) (stating that libelous speech is not protected by the Constitution but must not be used as a guise for punishing criticism).

n118. United States v. Stewart, No. 03 CR. 717(MGC), 2004 WL 113506, at 2 (S.D.N.Y. Jan. 26, 2004) (mem.).

n119. Ohralik v. Ohio State Bar Ass'n, 436 U.S. 447, 456 (1978) (citing Mills v. Elec. Auto-Lite Co., 396 U.S. 375 (1970)).

n120. Id. (citing Am. Column & Lumber Co. v. United States, 257 U.S. 377 (1921)).

n121. United States v. Longo, 70 F. Supp. 2d 225, 264 (W.D.N.Y. 1999) (holding that the proper remedy for evidence gained as a breach of the attorney-client privilege is suppression of the evidence).

n122. See Chemerinsky, supra note 112, at 695.

n123. My purpose at this stage of the analysis is merely to sketch the basic conceptual framework that courts should apply in approaching the intersection of privacy and speech. In Part III of this Article, I attempt to demonstrate in greater detail how this approach is consistent with the bulk of modern free speech jurisprudence, and how ordinary doctrinal tools can be applied to demonstrate the constitutionality of most meaningful regulatory responses to the database problem. Because doctrinal rules are only as good as the policies underlying them and the consequences they produce, in Part IV, I attempt a more abstract normative defense of the jurisprudential implications of my approach.

n124. See infra Part III.D.

n125. See infra notes 213-215 and accompanying text.

n126. See supra notes 62-69 and accompanying text.

n127. Eugene Volokh, The First Amendment: Problems, Cases and Policy Arguments 2 (2001).

n128. See Volokh, supra note 3, at 1084-88.

n129. See supra notes 107-111 and accompanying text.

n130. Schauer, supra note 98, at 1777-78.

n131. The scholarship of Eugene Volokh can be seen as trying to use existing doctrinal tools to bring these unappreciated or underappreciated contexts within the ambit of First Amendment protection. His response to my claim would presumably be "I am arguing that courts ought not ignore the First Amendment this way; when speech is being restricted based on its content, courts should explicitly explain why this restriction is permissible." Eugene Volokh, Speech as Conduct: Generally Applicable Laws, Illegal Courses of Conduct, "Situation-Altering Utterances," and the Uncharted Zones, 90 Cornell L. Rev. (forthcoming 2005) (manuscript at 58 n.212, on file with author); see also sources cited infra note 372 and accompanying text. To the extent that this is a normative argument rather than a descriptive one, I respond to it infra Part IV.

n132. Volokh, supra note 3, at 1098.

n133. Id. at 1087.

n134. For example, in his dissent from the denial of certiorari in the Trans Union case, Justice Kennedy noted that the law was unsettled about how to characterize the sale of a targeted marketing list containing the names and addresses of consumers. Trans Union LLC v. FTC, 536 U.S. 915, 916 (2002) (Kennedy, J., dissenting from denial of certiorari). Justice Kennedy did seem to hint that he thought the lists were entitled to some protection, but a dissent from a denial of certiorari has no precedential value. To the contrary, Kennedy's dissent reveals the confusion in this area of First Amendment law, as he acknowledges that the Court's plurality opinion in Dun & Bradstreet, Inc. v. Greenmoss Builders, Inc., 472 U.S. 749 (1985), is in some tension with his own views of the scope of heightened First Amendment protection.

n135. Schauer, supra note 98, at 1778.

n136. 376 U.S. 254 (1964).

n137. Melville B. Nimmer, The Right to Speak from Times to Time: First Amendment Theory Applied to Libel and Misapplied to Privacy, 56 Cal. L. Rev. 935, 942-43 (1968).

n138. Laurence H. Tribe, American Constitutional Law 792-93 (2d ed. 1988); David A. Anderson, Torts, Speech, and Contracts, 75 Tex. L. Rev. 1499, 1510 (1997).

n139. See, e.g., Bartnicki v. Vopper, 532 U.S. 514, 534 (2001) ("In this case, privacy concerns give way when balanced against the interest in publishing matters of public importance."). The Court also considers privacy (or at least the line between that which is public and that which is private) as a critical element in allocating the standard of review in defamation cases - public figures must plead and prove more elements than private figures who bring the action in order to recover for damage due to their reputations. Compare Sullivan, 376 U.S. at 279-80 (requiring a public figure to prove actual malice to recover for defamation), with Gertz v. Robert Welch, Inc., 418 U.S. 323, 347 (1974) (requiring private figures to prove only something more than strict liability to recover damages for actual injury).

n140. Volokh, supra note 3, at 1052.

n141. Id.

n142. See, e.g., Cent. Hudson Gas & Elec. Corp. v. Pub. Serv. Comm'n, 447 U.S. 557, 563-64 (1980) (stating that commercial speech receives intermediate scrutiny); United States v. O'Brien, 391 U.S. 367, 382 (1968) (applying intermediate scrutiny to a conviction for burning a draft card).

n143. See, e.g., Virginia v. Black, 538 U.S. 343, 359 (2003) ("Threats of violence are outside the First Amendment ... ."); R.A.V. v. City of St. Paul, 505 U.S. 377, 388 (1992) (same); Time, Inc. v. Hill, 385 U.S. 374, 389-90 (1967) (libelous statements made with "calculated falsehood"); Roth v. United States, 354 U.S. 476, 485 (1957) (obscenity); Chaplinsky v. New Hampshire, 315 U.S. 568, 572 (1942) ("fighting words").

n144. See, e.g., White, supra note 8; Tony A. Freyer, The First Amendment and World War II, [1996] 1 J. Sup. Ct. Hist. 83; Neil M. Richards, The "Good War," the Jehovah's Witnesses, and the First Amendment, 87 Va. L. Rev. 781, 794 (2001) (reviewing Shawn Francis Peters, Judging Jehovah's Witnesses: Religious Persecution and the Dawn of the Rights Revolution (2000)).

n145. 315 U.S. 568 (excluding from First Amendment protection ""fighting' words - those which by their very utterance inflict injury or tend to incite an immediate breach of the peace.").

n146. See, e.g., Texas v. Johnson, 491 U.S. 397, 409 (1989); City of Houston v. Hill, 482 U.S. 451, 462-63 (1987); Hess v. Indiana, 414 U.S. 105, 107 (1973); Norwell v. City of Cincinnati, 414 U.S. 14, 16 (1973); Lewis v. City of New Orleans, 408 U.S. 913 (1972); Rosenfeld v. New Jersey, 408 U.S. 901, 905 (1972); Gooding v. Wilson, 405 U.S. 518, 528 (1972); Cohen v. California, 403 U.S. 15, 20 (1971); Street v. New York, 394 U.S. 576, 592 (1969).

n147. Gooding, 405 U.S. 518.

n148. Id. at 528.

n149. 316 U.S. 52 (1942).

n150. Id. at 54-55; see also Breard v. Alexandria, 341 U.S. 622, 645 (1951) (reaffirming Chrestensen as applied to a prohibition against door-to-door solicitation of magazine subscriptions).

n151. See Va. State Bd. of Pharm. v. Va. Citizens Consumer Council, Inc., 425 U.S. 748, 770 (1976).

n152. 447 U.S. 557 (1980).

n153. See, e.g., Thompson v. W. States Med. Ctr., 535 U.S. 357, 367-68 (2002) (noting that "several Members of the Court have expressed doubts about the Central Hudson analysis and whether it should apply in particular cases" (citing Greater New Orleans Broad. Assn. v. United States, 527 U.S. 173, 197 (1999) (Thomas, J., concurring))); 44 Liquormart, Inc. v. Rhode Island, 517 U.S. 484, 501, 510-14 (1996) (Stevens, J.) (joined by Kennedy, Souter, and Ginsburg, JJ.); id. at 517 (Scalia, J., concurring in part and concurring in the judgment); id. at 518 (Thomas, J., concurring in part and concurring in the judgment); see also William Van Alstyne, To What Extent Does the Power of Government to Determine the Boundaries and Conditions of Lawful Commerce Permit Government to Declare Who May Advertise and Who May Not?, 51 Emory L.J. 1513, 1545 & n.84 (2002).

n154. Schwartz, supra note 71, at 1563-64.

n155. Solove, supra note 71, at 981.

n156. Id.

n157. Id. at 976-77.

n158. See supra notes 127-132 and accompanying text.

n159. Solove, supra note 71, at 1031.

n160. Id. at 1026.

n161. Id. at 1027.

n162. Privacy scholars have struggled for decades to come up with a workable definition of privacy and have failed to reach a consensus. See Solove, supra note 10, at 1088 (collecting sources).

n163. See Doe v. High-Tech Inst., Inc., 972 P.2d 1060, 1067 (Colo. Ct. App. 1998) (noting that the "vast majority of courts in other jurisdictions" have recognized not only other types of privacy claims, but also specifically "intrusion upon seclusion" claims). Indeed, with Minnesota most recently adopting the privacy tort via the common law in 1998, see Lake v. Wal-Mart Stores Inc., 582 N.W.2d 231, 235 (Minn. 1998), only North Dakota and Wyoming have never recognized a cause of action for invasion of privacy, see O'Neil, supra note 57, at 77.

n164. See William L. Prosser, Privacy, 48 Cal. L. Rev. 383, 388-89 (1960); Warren & Brandeis, supra note 4. The torts themselves, however, were as much the creation of Prosser as of Warren and Brandeis. See infra notes 276-287 and accompanying text.

n165. Restatement (Second) of Torts 652B (1977).

n166. E.g., Birnbaum v. United States, 436 F. Supp. 967, 978 (E.D.N.Y. 1977) (recognizing an invasion of privacy when the Central Intelligence Agency opened and copied plaintiff's mail).

n167. E.g., McDonald's Corp. v. Levine, 439 N.E.2d 475, 480 (Ill. App. Ct. 1982) (stating that violations of the Illinois Eavesdropping Act of 1977 can constitute an actionable intrusion upon seclusion); Hamberger v. Eastman, 206 A.2d 239, 244 (N.H. 1964) (holding that placing a listening device in plaintiff's bedroom is an invasion of privacy).

n168. E.g., Ford Motor Co. v. Williams, 132 S.E.2d 206, 211-12 (Ga. Ct. App. 1963) (establishing liability for nonconsensual entrance into plaintiff's home, even though no one was there); Gerard v. Parish of Jefferson, 424 So. 2d 440, 445 (La. Ct. App. 1982) ("The right to privacy includes the right to be free from unwarranted

intrusion into one's own quarters.").

n169. E.g., Stevenson v. Precision Standard, Inc., 762 So. 2d 820, 826 (Ala. 1999) (noting that sexual harassment could rise to the level of intrusion upon seclusion if it includes "egregious inquiries into one's sex life coupled with intrusive and coercive sexual demands"); Philips v. Smalley Maint. Servs. Inc., 435 So. 2d 705, 711 (Ala. 1983) (defendant's conduct was "an "examination' into [plaintiff's] "private concerns,' that is, improper inquiries into her personal sexual proclivities and personality"); Pearson v. Kancilia, 70 P.3d 594 (Colo. Ct. App. 2003).

n170. E.g., Carey v. Statewide Fin. Co., 223 A.2d 405, 406-07 (Conn. Cir. Ct. 1966) (holding that creditor's harassing phone calls to plaintiff's home and the hospital "is actionable as an invasion of plaintiff's right to privacy"); Housh v. Peth, 133 N.E.2d 340, 344 (Ohio 1956) (holding that creditors who harassed a debtor with repeated phone calls at late hours for a three-week period were liable for intrusion upon seclusion).

n171. E.g., Nader v. Gen. Motors Corp., 255 N.E.2d 765, 771 (N.Y. 1970) (noting that surveillance may be "so overzealous as to render it actionable"); Galella v. Onassis, 353 F. Supp. 196, 227-28 (S.D.N.Y. 1972) (holding that a defendant who ignored restraining orders to photograph a plaintiff and the plaintiff's family violated the invasion of privacy).

n172. E.g., Harkey v. Abate, 346 N.W.2d 74, 76 (Mich. Ct. App. 1983) (installation of see-through panels in women's restroom). See generally Richard C. Turkington & Anita A. Allen, Privacy Law: Cases and Materials (1999) (collecting cases).

n173. Pioneer Hi-Bred Int'l v. Holden Found. Seeds, Inc., 35 F.3d 1226, 1238 n.42 (8th Cir. 1994).

n174. The Supreme Court has noted that the need to protect information from industrial espionage is one of the core interests that the federal Wiretap Act was enacted to address. Bartnicki v. Vopper, 532 U.S. 514, 530 n.16 (2001).

n175. 18 U.S.C.A. 2511 (West 2000 & Supp. 2004).

n176. Earley v. Executive Bd. of the United Transp. Union, 957 F. Supp. 997 (N.D. Ohio 1996) (surreptitious tape recording of arbitration panel).

n177. Cross v. Ala. State Dep't of Mental Health & Mental Retardation, 49 F.3d 1490 (11th Cir. 1995).

n178. Glazner v. Glazner, 347 F.3d 1212, 1221 (11th Cir. 2003) (recording wife's telephone conversations without her consent); United States v. Dossey, 66 Fed. Appx. 528, 531 (6th Cir. 2003) (hidden recording device attached to commercial establishment's telephones); Bess v. Bess, 929 F.2d 1332, 1336 (8th Cir. 1991) (tape recording wife's telephone conversations); Dunn v. Blue Ridge Tel. Co., 868 F.2d 1578, 1582-83 (11th Cir. 1989) (employer monitoring telephone call); Epps v. St. Mary's Hosp. of Athens, 802 F.2d 412 (11th Cir. 1986) (fellow employee monitoring telephone call); Watkins v. L.M. Berry & Co., 704 F.2d 577 (11th Cir. 1983) (employer monitoring telephone call); Goodspeed v. Harman, 39 F. Supp. 2d 787, 792-94 (N.D. Tex. 1999) (intentional eavesdropping on neighbor's cordless telephone calls using a police scanner); In re State Police Litig., 888 F. Supp. 1235 (D. Conn. 1995) (recordings of telephone conversations made by police commission, which did not listen to them); George v. Carusone, 849 F. Supp. 159, 164 (D. Conn. 1994) (same); Pascale v. Carolina Freight Carrier Corp., 898 F. Supp. 276, 282 (D.N.J. 1995) (employer's workplace recording of employees' telephone conversations with wives); Biton v. Menda, 812 F. Supp. 283, 283 (D.P.R. 1993) (nonconsensual recording of telephone conversation with stockbroker).

n179. Jacobson v. Rose, 592 F.2d 515 (9th Cir. 1978).

n180. E.g., Cal. Penal Code 631 (West 1999); Fla. Stat. Ann. 934.10 (West 2001); Mass. Ann. Laws ch. 272, 99Q (Law. Co-op. 2004); Minn. Stat. Ann. 626A.13, 626A.32 (West 2003); N.Y. Penal Law 250 (McKinney 2000); Wash. Rev. Code Ann. 9.73.060 (West 2003).

n181. The Massachusetts wiretapping statute, Mass. Ann. Laws ch. 272, 99, has been held more restrictive than ECPA and, thus, not subject to preemption by the federal law. United States v. Smith, 726 F.2d 852, 862 (1st Cir. 1984); accord Minn. Stat. Ann. 626A.13, 626A.32 (unlike ECPA, provides civil remedy for violations involving intrastate communications).

n182. See E. Allan Farnsworth, Contracts 4.28 (3d ed. 1999); see also Restatement (Second) of Contracts 159-173 (1981) (discussing elements of fraudulent misrepresentations); Restatement (Second) of Torts 525-548A (1977) (same).

n183. See Minnesota ex rel. Hatch v. Fleet Mortgage Corp., 158 F. Supp. 2d 962, 966-68 (D. Minn. 2001) (holding that a bank's failure to disclose to customers that it planned to share customer information with telemarketers stated a claim under the UDTPA and state fraud law).

n184. Federal Trade Comm'n Act 5, 15 U.S.C. 45 (2000). The FTC has indicated that it understands the Act to grant it such authority and has brought actions pursuant to this authority. See, e.g., Gateway Learning Corp., No. C-4120 (FTC Sept. 10, 2004), available at http://www.ftc.gov/os/caselist/0423047/0423047.htm.

n185. 15 U.S.C.A. 1681b(b) (West 1997 & Supp. 2004). See generally Solove & Rotenberg, supra note 82, at 520-21.

n186. 18 U.S.C.A. 1030(a)(2)(C) (West 2000 & Supp. 2004).

n187. Id. 2510(4), 2511(1)(a).

n188. Id. 2511(2)(d).

n189. Id. 2511(4)(a) (authorizing imprisonment for up to five years for violations).

n190. Id. 2520(c)(2). Successful plaintiffs can obtain damages equal to the greater of (1) the sum of the actual damages and the defendant's profit as a result of the violation or (2) statutory damages equal to the greater of $ 100 per day of violation or $ 10,000. Id.

n191. 15 U.S.C. 6501-6506 (2000).

n192. For example, in 1998 the FTC filed a complaint against a company called GeoCities after it "misrepresented the purposes for which it was collecting personal identifying information from children and adults." GeoCities and the FTC agreed to settle later that year. See Press Release, Fed. Trade Comm'n, Internet

Site Agrees to Settle FTC Charges of Deceptively Collecting Personal Information in Agency's First Internet Privacy Case: Commission Establishes Strong Mechanisms for Protecting Consumers' Privacy Online (Aug. 13, 1998), available at http://www.ftc.gov/opa/1998/08/geocitie.htm. Although the settlement has been criticized by scholars for being little more than a slap on the wrist, see, e.g., Paul M. Schwartz, Privacy and Democracy in Cyberspace, 52 Vand. L. Rev. 1609, 1637-38 (1999), the larger point is that information collection regulation of this sort is already within the purview of the FTC and is not considered to be constitutionally infirm. More recently, the FTC has brought charges against a company called Gateway Learning Corporation for allegedly renting out customer information collected from its web site to direct marketers, despite promises to the contrary in its privacy policy. Gateway Learning Corp., No. C-4120 (FTC Sept. 10, 2004), available at http://www.ftc.gov/os/caselist/0423047/0423047.htm.

n193. See Steven Hetcher, The FTC as Internet Privacy Norm Entrepreneur, 53 Vand. L. Rev. 2041, 2046-47 (2000).

n194. Cohen v. Cowles Media Co., 501 U.S. 663, 670 (1991).

n195. Hudgens v. NLRB, 424 U.S. 507, 521 (1976).

n196. See id.; see also Cent. Hardware Co. v. NLRB, 407 U.S. 539, 547 (1972); Lloyd Corp. v. Tanner, 407 U.S. 551, 568 (1972). One exception to this rule, not implicated in the database context, is that the First Amendment does apply to speech restrictions imposed by private actors who have assumed the performance of substantial government functions - for example by operating a "company town." Hudgens, 424 U.S. at 514-21; Marsh v. Alabama, 326 U.S. 501, 509 (1946).

n197. See O'Neil, supra note 57, at 76-90; see also id. at 176-78 (collecting cases).

n198. See, e.g., Galella v. Onassis, 487 F.2d 986, 995 (2d Cir. 1973) (denying paparazzi First Amendment immunity from liability if they go "beyond the reasonable bounds of news gathering"); Dietemann v. Time, Inc., 449 F.2d 245, 249 (9th Cir. 1971) (noting that the First Amendment provides the news media no license to trespass or intrude into the dwelling of another); Shulman v. Group W Prods., Inc., 955 P.2d 469, 477, 493 (Cal. 1998) (finding no First Amendment immunity from tort liability for media attempting to gather material for a potentially newsworthy story); Miller v. Nat'l Broad. Co., 232 Cal. Rptr. 668, 684 (Ct. App. 1986) (same); Prahl v. Brosamle, 295 N.W.2d 768, 781 (Wis. Ct. App. 1980) (finding no First Amendment privilege to trespass).

n199. 194 F.3d 505 (4th Cir. 1999).

n200. Id. at 510.

n201. See id. at 517 (collecting cases).

n202. Id. at 517-18.

n203. Thus, in Food Lion, although the panel divided on whether the elements of the various state law torts had been met, compare id. at 519-20, with id. at 524 (Niemeyer, J., concurring in part and dissenting in part), the panel was unanimous in rejecting the media defendants' argument that the First Amendment created a press privilege to commit torts in the process of newsgathering, id. at 520-22; id. at 524 (Niemeyer, J., concurring in part and dissenting in part).

n204. If a law singles out the press for special, unfavorable treatment, it is likely to be invalidated. See, e.g., Minneapolis Star & Tribune Co. v. Minn. Comm'r of Revenue, 460 U.S. 575, 592-93 (1983) (holding that a special use tax on ink and paper levied only against periodic publications violates the First Amendment).

n205. 408 U.S. 665 (1972).

n206. Id. at 691; see also Konigsberg v. State Bar of Cal., 366 U.S. 36, 50-51 (1961) ("General regulatory statutes, not intended to control the content of speech but incidentally limiting its unfettered exercise, have not been regarded as the type of law the First or Fourteenth Amendment forbade Congress or the States to pass, when they have been found justified by subordinating valid governmental interests ... .").

n207. 501 U.S. 663 (1991).

n208. Id. at 669.

n209. 532 U.S. 514 (2001).

n210. Id. at 532 n.19.

n211. N.Y. Times Co. v. United States, 403 U.S. 713, 730 (1971) (White, J., concurring) (stating that several criminal laws protecting government property and preserving government secrets, although not before the court, "are of very colorable relevance to the apparent circumstances of these cases").

n212. 526 U.S. 603 (1999).

n213. Arcara v. Cloud Books, Inc., 478 U.S. 697, 706 (1986).

n214. See generally Arcara, 478 U.S. 697. See also City of Ladue v. Gilleo, 512 U.S. 43, 54-55 (1994) (holding that an ordinance prohibiting residents from installing yard signs warrants heightened First Amendment review because it closed off an entire important medium for expression); United States v. O'Brien, 391 U.S. 367, 382 (1968) (applying intermediate scrutiny to a conviction for burning a draft card because of the potential impact of application of the conduct rule to important political expression).

n215. See Rodney A. Smolla, Privacy and the First Amendment Right to Gather News, 67 Geo. Wash. L. Rev. 1097, 1128 (1999).

n216. Cf. Food Lion, Inc. v. Capital Cities/ABC, Inc., 194 F.3d 505, 520 (4th Cir. 1999) (noting that application of ordinary private law rules to newsgathering does not violate the First Amendment, even though newsgathering by the media is a protected activity under the Press Clause of the First Amendment).

n217. I discuss information disclosure rules infra Part III.C.

n218. See Peter P. Swire, The Surprising Virtues of the New Financial Privacy Law, 86 Minn. L. Rev. 1263, 1294-1314 (2002).

n219. See generally Swire, supra note 218.

n220. Concern about the improper use of social security numbers dates back at least to the 1973 Department of Health, Education, and Welfare report. U.S. Dep't of Health, Educ. & Welfare, supra note 76.

n221. See, e.g., Mass. Ann. Laws ch. 175I, 13 (Law. Co-op. 1996) (regulating the use of confidential information in insurance transactions).

n222. The current Model Rules of Professional Conduct impose both a duty of confidentiality and a duty not to use information, which varies depending on whether the client is a "prospective client," current client, or former client. Model Rules of Prof'l Conduct R. 1.18 (2003) (prospective clients); R. 1.6, 1.8(b) (current clients); R. 1.9(c) (former clients).

n223. See, e.g., Civil Rights Act of 1964, tit. VII, 42 U.S.C. 2000e-2(a) (2000) ("It shall be an unlawful employment practice for an employer - (1) to fail or refuse to hire or discharge any individual, or otherwise to discriminate against any individual with respect to his compensation, terms, conditions, or privileges of employment, because of such individual's race, color, religion, sex, or national origin ... ."); id. tit. IX, 20 U.S.C. 1681(a) (2000) ("No person in the United States shall, on the basis of sex, be excluded from participation in, be denied the benefits of, or be subjected to discrimination under any education program or activity receiving Federal financial assistance ... ."); Americans With Disabilities Act, 42 U.S.C. 12112(a) ("No covered entity shall discriminate against a qualified individual with a disability because of the disability of such individual in regard to job application procedures, the hiring, advancement, or discharge of employees, employee compensation, job training, and other terms, conditions, and privileges of employment."); see also Age Discrimination in Employment Act, 29 U.S.C. 623 (2000) ("It shall be unlawful for an employer - (1) to fail or refuse to hire or to discharge any individual or otherwise discriminate against any individual with respect to his compensation, terms, conditions, or privileges of employment, because of such individual's age ... .").

n224. 15 U.S.C.A. 1681b(a)(3) (West 1997 & Supp. 2004).

n225. Id. 1681b(b). See generally Solove & Rotenberg, supra note 82, at 520-21.

n226. See Restatement (Third) of Unfair Competition 39 (1995) ("A trade secret is any information that can be used in the operation of a business or other enterprise and that is sufficiently valuable and secret to afford an actual or potential economic advantage over others.").

n227. 35 U.S.C. 271(a) (2000); see also Neff Instrument Corp. v. Cohu Elecs., Inc., 269 F.2d 668, 673 (9th Cir. 1959) (holding the bare manufacture of a single device protected by a patent is infringement, even if device is never used or sold).

n228. See, e.g., Cal. Civ. Code 1798.85(a)(3) (West Supp 2005) (prohibiting the use of social security numbers in unsecure internet transmissions).

n229. See, e.g., Ohio Rev. Code Ann. 4501.27(A) (West 1999 & Supp. 2004) (regulating the use of personal information "obtained in connection with a motor vehicle record").

n230. See, e.g., 13 U.S.C. 8(c) (2000) (barring use of census information "to the detriment of any respondent").

n231. 18 U.S.C.A. 2511(1)(c) (West 2000 & Supp. 2004).

n232. S. Rep. No. 90-1097, at 67 (1968), reprinted in 1968 U.S.C.C.A.N. 2112, 2154; see also Bartnicki v. Vopper, 532 U.S. 514, 526-27 & 527 n.10 (2001).

n233. Thompson v. Dulaney, 838 F. Supp. 1535, 1547 (D. Utah 1993) (holding such activities to constitute a violation of ECPA separate from the interception itself).

n234. See Bartnicki, 532 U.S. at 527 n.10 (citing Brief for United States at 24).

n235. Dorris v. Absher, 959 F. Supp. 813, 815-16, 819 (M.D. Tenn. 1997).

n236. Bess v. Bess, 929 F.2d 1332, 1334 (8th Cir. 1991).

n237. Berry v. Funk, 146 F.3d 1003, 1011-13 (D.C. Cir. 1998) (knowing use of unlawfully intercepted communications by Inspector General in investigations); Chandler v. United States Army, 125 F.3d 1296, 1298-1302 (9th Cir. 1997) (use by military of taped conversation in adultery investigation); In re Grand Jury, 111 F.3d 1066, 1068, 1075 (3d Cir. 1997) (disclosure of an illegally recorded conversation to grand jury, even where such disclosure would be in compliance with subpoena).

n238. See Fultz v. Gilliam, 942 F.2d 396, 400 n.4 (6th Cir. 1991) (envisioning extortionary use of intercepted communications as violating ECPA).

n239. 532 U.S. 514, 524-27 (2001); see also 18 U.S.C. 2511(1)(c) (2000) (disclosure); 2511(1)(d) (use).

n240. Bartnicki, 532 U.S. at 526-27 (footnote omitted).

n241. Id. at 526-27 & 527 n.10 (citing favorably a long list of such examples proffered by the Solicitor General); see also id. at 529. The case states:

The government identifies two interests served by the statute - first, the interest in removing an incentive for parties to intercept private conversations, and second, the interest in minimizing the harm to persons whose conversations have been illegally intercepted. We assume that those interests adequately justify the [use] prohibition in 2511(1)(d) against the interceptor's own use of information that he or she acquired by violating 2511(1)(a) ... .

Id.

n242. See Brief of Appellant U.S. West, Inc. at 6, U.S. West, Inc. v. FCC, 182 F.3d 1224 (10th Cir. 1999) (No. 98-3451).

n243. U.S. West, 182 F.3d at 1232.

n244. Id. at 1232-33.

n245. Id. at 1233 n.4.

n246. Id. at 1237-38.

n247. Id. at 1238-39.

n248. Id. at 1235-36.

n249. See Swire, supra note 218, at 1293-1314.

n250. 16 C.F.R. 310.4(b)(1)(iii)(B) (2004) (defining "an abusive telemarketing act or practice" as a "telephone call to a person when ... that person's telephone number is on the "do-not-call' registry, maintained by the Commission, of persons who do not wish to receive outbound telephone calls to induce the purchase of goods or services").

n251. See, e.g., Volokh, supra note 3, at 1057.

n252. See Am. Med. Ass'n, Code of Medical Ethics 5.05 (1999) ("The physician should not reveal confidential communications or information without the express consent of the patient, unless required to do so by law.").

n253. See supra note 222 and accompanying text.

n254. See, e.g., Upjohn Co. v. United States, 449 U.S. 383, 389 (1981) ("The attorney-client privilege is the oldest of the privileges for confidential communication known to the common law."); see also Cal. Evid. Code 954 (West 1995) (codifying attorney-client privilege); N.Y. C.P.L.R. 4503 (McKinney 1992 & Supp. 2004) (same).

n255. See, e.g., Cal. Evid. Code 994 (codifying doctor-patient privilege); N.Y. C.P.L.R. 4504 (same); Wis. Stat. Ann. 905.04 (West 2000 & Supp. 2003) (same).

n256. See Graham C. Lilly, An Introduction to the Law of Evidence 442-51 (3d ed. 1996).

n257. Jaffee v. Redmond, 518 U.S. 1, 15-17 (1996) (recognizing psychotherapist-patient privilege with licensed psychologists, psychiatrists, and "licensed social workers in the course of psychotherapy"); see also Cal. Evid. Code 1014 (West 1995 & Supp. 2005) (codifying psychotherapist-patient privilege); Fla. Stat. Ann. 90.503 (West 1999 & Supp. 2005) (same); Mass. Ann. Laws ch. 233, 20B (Law. Co-op. 2004) (same).

n258. Some states recognize a priest-penitent privilege. See, e.g., Cal. Evid. Code 1033-1034; Ind. Code Ann. 34-46-3-1 (Michie 1998); Mass. Ann. Laws ch. 233, 20A (Law. Co-op. 2000). Others recognize an accountant-client privilege. See, e.g., Fla. Stat. Ann. 473.316 (West 2001); Ga. Code Ann. 43-3-32 (2002); 225 Ill. Comp. Stat. Ann. 450/27 (West 1993).

n259. See Restatement (Second) of Agency 395 (1958) ("Unless otherwise agreed, an agent is subject to a duty to the principal not to use or to communicate information confidentially given him by the principal or acquired by him during the course of or on account of his agency or in violation of his duties as agent ... .").

n260. See supra note 226.

n261. For example, California prohibits any person from "publicly posting or publicly displaying in any manner an individual's social security number." Cal. Civ. Code 1798.85(a)(1) (West Supp 2005).

n262. 18 U.S.C. 1831-1832 (2000).

n263. E.g., SEC Regulation FD, 17 C.F.R. 243.100 (2004) (preventing the selective disclosure of "material nonpublic information" by issuers of securities to selected securities traders rather than to the public as a whole); see also Schauer, supra note 98, at 1778-83 (collecting other examples).

n264. Gramm-Leach-Bliley Act, 15 U.S.C. 6801-6809 (2000).

n265. Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (codified in scattered sections of 18, 26, 29, and 42 U.S.C.); see also Privacy of Individually Identifiable Health Information, 45 C.F.R. 164.500-.534.

n266. Video Privacy Protection Act, 18 U.S.C.A. 2710-2711 (West 2000 & Supp. 2004); Cable Communications Policy Act, 47 U.S.C.A. 551 (West 2001 & Supp. 2004).

n267. 18 U.S.C.A. 2511(1) (West 2000 & Supp. 2004).

n268. Id. 2702.

n269. See Schauer, supra note 98, at 1777-84; cf. Richard A. Epstein, Privacy, Publication, and the First Amendment: The Dangers of First Amendment Exceptionalism, 52 Stan. L. Rev. 1003, 1035-47 (2000) (discussing trade secrets in the First Amendment context).

n270. See Bartnicki v. Vopper, 532 U.S. 514, 527-28 (2001).

n271. See id. at 526-28 (holding that a radio station cannot be prohibited from publishing newsworthy

information of public concern, even where such information had been illegally obtained by a third party); Fla. Star v. B.J.F., 491 U.S. 524, 526 (1989) (holding that a state statute prohibiting the publication of the name of a rape victim was unconstitutional as applied to a newspaper that had obtained the name from a "publicly released police report"); Smith v. Daily Mail Publ'g Co., 443 U.S. 97 (1979) (holding the First Amendment prohibits a state from punishing a newspaper for publishing the name of a juvenile murder suspect because the press lawfully obtained the information); Okla. Publ'g Corp. v. Okla. County Dist. Court, 430 U.S. 308 (1977) (holding the First Amendment prevents a state court from prohibiting the media from publishing the name of a juvenile in a proceeding that a reporter attended); Cox Broad. Corp. v. Cohn, 420 U.S. 469 (1975) (holding the name of a rape victim obtained by the press from public records cannot be prevented from being published by statute or made the basis for liability under the nondisclosure tort).

n272. 491 U.S. 524 (1989).

n273. Id. at 541.

n274. Volokh, supra note 3, at 1051; see also Cate, supra note 1, at 70.

n275. See, e.g., Singleton, supra note 54, at 132-53.

n276. See The Right to Privacy in Nineteenth Century America, supra note 17 (arguing that the right of privacy identified by Warren and Brandeis was predated by the broad protection given under nineteenth century law to private property, confidential communications, and personal information).

n277. Warren & Brandeis, supra note 4, at 195.

n278. Id. at 213-20.

n279. See Richards, supra note 144, at 781-82 (noting that "between 1937 and 1954 ... the Court decided a number of critical First Amendment cases that laid the doctrinal and conceptual foundation for much of modern free speech and free exercise of religion jurisprudence").

n280. See G. Edward White, Tort Law in America: An Intellectual History 174 (expanded ed. 2003) (citing Roberson v. Rochester Folding Box Co., 64 N.E. 442 (N.Y. 1902), and Pavesich v. New England Life Ins. Co., 50 S.E. 68 (Ga. 1904)).

n281. See White, supra note 280, at 173-76.

n282. William L. Prosser, Handbook of the Law of Torts 637-40 (2d ed. 1955).

n283. William L. Prosser, Handbook of the Law of Torts 1050-51 (1941).

n284. See White, supra note 280, at 173, 175-76.

n285. See Prosser, supra note 164, at 389, 422; see also White, supra note 280, at 176.

n286. See cases cited supra note 271.

n287. See, e.g., Edward J. Bloustein, The First Amendment and Privacy: The Supreme Court Justice and the Philosopher, 28 Rutgers L. Rev. 41 (1974); Peter B. Edelman, Free Press v. Privacy: Haunted by the Ghost of Justice Black, 68 Tex. L. Rev. 1195 (1990); Paul Gewirtz, Privacy and Speech, 2001 Sup. Ct. Rev. 139; Harry Kalven, Jr., Privacy in Tort Law - Were Warren and Brandeis Wrong?, 31 Law & Contemp. Probs. 326, 366 (1966); Nimmer, supra note 137, at 935; Solove, supra note 71, at 972-73; Zimmerman, supra note 4, at 341-62.

n288. See supra Part II.B.

n289. See supra notes 252-269.

n290. Bartnicki v. Vopper, 532 U.S. 514, 529 (2001) ("The sensitivity and significance of the interests presented in clashes between [the] First Amendment and privacy rights counsel relying on limited principles that sweep no more broadly than the appropriate context of the instant case." (quoting Fla. Star v. B.J.F., 491 U.S. 524, 532-33 (1989))).

n291. Id.

n292. See, e.g., Cohen, supra note 47, at 1414, 1417; Edelman, supra note 287, at 1229-30; Solove, supra note 71, at 1013-30.

n293. Cf. Warren & Brandeis, supra note 4, at 214-16.

n294. See Solove, supra note 71, at 1000-30 (collecting sources).

n295. See, e.g., Bartnicki, 532 U.S. at 529 (noting "this Court's repeated refusal to answer categorically whether truthful publication may ever be punished consistent with the First Amendment").

n296. 472 U.S. 749 (1985).

n297. Id. at 760.

n298. See, e.g., Katy J. Lewis, Comment, Bartnicki v. Vopper: A New Bully in the Schoolyard of Private Expression, 70 Tenn. L. Rev. 859, 886 (2003) (arguing that the Court diminished individual privacy rights in Bartnicki).

n299. Bartnicki, 532 U.S. at 535; see also Glickman v. Wileman Bros. & Elliott, Inc., 521 U.S. 457 (1997)

(holding the First Amendment analysis inapplicable to businesses' complaint of mandatory assessment used for generic pro-industry advertising); Cent. Hudson Gas & Elec. Corp. v. Pub. Serv. Comm'n, 447 U.S. 557, 561-63 (1980) (granting intermediate scrutiny to "expression related solely to the economic interests of the speaker and its audience").

n300. See Rodney A. Smolla, Information as Contraband: The First Amendment and Liability for Trafficking in Speech, 96 Nw. U. L. Rev. 1099 (2002).

n301. See Volokh, supra note 3, at 1057.

n302. 501 U.S. 663 (1991).

n303. Id. at 669-70; see also id. at 670 ("The publisher of a newspaper has no special immunity from the application of general laws. He has no special privilege to invade the rights and liberties of others." (quoting Associated Press v. NLRB, 301 U.S. 103, 132-33 (1937))).

n304. Volokh, supra note 3, at 1057-58.

n305. Id. at 1058-60.

n306. Id. at 1061.

n307. Id. at 1061-62.

n308. See Schwartz, supra note 71, at 1569-71.

n309. Volokh, supra note 3, at 1060 n.37.

n310. Id. at 1059 n.35.

n311. See, e.g., Hetcher, supra note 193.

n312. Volokh, supra note 3, at 1058-62 & n.42 (citing Cohen v. Cowles Media Co., 501 U.S. 663, 671 (1991)).

n313. See Roger E. Schechter & John R. Thomas, Intellectual Property: The Law of Copyrights, Patents and Trademarks 24.3 (2003).

n314. See Farnsworth, supra note 182, 1.10.

n315. See id. 4.28.

n316. Children's Privacy Protection Act, 15 U.S.C. 6501-6506 (2000).

n317. See Froomkin, supra note 29, at 1502-03.

n318. See id. at 1502.

n319. See infra Part IV.B.

n320. See Restatement (Second) of Contracts 90 cmt. a (1981) ("Obligations and remedies based on reliance are not peculiar to the law of contracts. This Section is often referred to in terms of "promissory estoppel,' a phrase suggesting an extension of the doctrine of estoppel.").

n321. Although it did not say so expressly, the Court's rejection of the claim made by Justice Souter in dissent that its holding would "inhibit truthful reporting," Cohen v. Cowles Media Co., 501 U.S. 633, 671 (1991), suggests that the Court determined that promissory estoppel did not have a significant impact on First Amendment values so as to subject it to intermediate scrutiny under Arcara/O'Brien. See supra notes 213-214 and accompanying text.

n322. 467 U.S. 20 (1984).

n323. Lucas A. Powe, Jr., The Fourth Estate and the Constitution 176 (1991).

n324. For example, in Cox Broadcasting Corp. v. Cohn, the Court stated:

Appellee has not contended that the name was obtained in an improper fashion or that it was not on an official court document open to public inspection. Under these circumstances, the protection of freedom of the press provided by the First and Fourteenth Amendments bars the State of Georgia from making appellants' broadcast the basis of civil liability.

420 U.S. 469, 496-97 (1975); see also Bartnicki v. Vopper, 532 U.S. 514, 527-29 (2001) (same); Fla. Star v. B.J.F., 491 U.S. 524, 541 (1989) (same); Smith v. Daily Mail Publ'g Co., 443 U.S. 97, 105-06 (1979) (same); Okla. Publ'g Co. v. Okla. County Dist. Court, 430 U.S. 308, 311-12 (1977) (same).

n325. Cf. Bartnicki, 532 U.S. at 532 & n.19.

n326. Volokh, supra note 3, at 1058.

n327. See supra notes 213-214 and accompanying text.

n328. See supra note 204.

n329. Cf. Schauer, supra note 98. In a thoughtful forthcoming article, Eugene Volokh makes the claim that the concept of generally applicable laws is insufficient to protect important First Amendment values from abridgement. In particular, he argues that it is not enough to uphold a law simply because it is content neutral on its face, because such rules can be content based as applied, for example to advocacy of illegal conduct. Volokh, supra note 131 (manuscript at 11). It is difficult and perhaps unfair to take issue with arguments that have not yet been published, but I believe that Volokh's assertion is inapplicable to my arguments here for three reasons. First, to the extent he argues that current doctrine underprotects First Amendment values, this does not conflict with my claim here that ordinary doctrinal tools can be used to sustain the constitutionality of a wide variety of nondisclosure and other privacy rules. Indeed, Volokh's dissatisfaction with the strictness of current doctrine in this area perhaps supports my claim that the First Amendment critics overstate the power of the First Amendment when they make normative claims about its applicability to privacy rules. Second, because the subversive advocacy cases are some distance removed from commercial database nondisclosure rules in terms of their proximity to the core of what the First Amendment protects, his critique does not speak to the privacy context, but rather to matters of indisputable public concern. Third, to the extent we probably do disagree about the breadth of the Cohen v. Cowles Media principle, I believe that my interpretation of this rather murky area of the jurisprudence is sufficiently speech-protective because heightened scrutiny is still retained for generally applicable laws that have a significant impact upon expressive activity. See supra notes 203-206 and accompanying text. Our ultimate disagreement may be simply one regarding the expressive content of databases, which I tend to treat as warranting lower scrutiny for reasons I develop further infra Part IV.

n330. See supra notes 150-153 and accompanying text.

n331. See Kang, supra note 10, at 1202.

n332. 410 U.S. 113 (1973).

n333. 381 U.S. 479 (1965).

n334. See Kang, supra note 10, at 1202.

n335. Id. at 1205-17.

n336. See, e.g., Kyllo v. United States, 533 U.S. 27 (2001) (holding that the well-established residential privacy of the home embodied in the Fourth Amendment prevents police from using thermal imagers from public streets to view into homes); Wilson v. Layne, 526 U.S. 603, 610 (1999) ("The Fourth Amendment embodies the centuries-old principle of respect for the privacy of the home ... .").

n337. See, e.g., Lawrence v. Texas, 539 U.S. 558, 562 (2003). The Lawrence Court stated:

In our tradition the State is not omnipresent in the home. And there are other spheres of our lives and existence, outside the home, where the State should not be a dominant presence. Freedom extends beyond spatial bounds. Liberty presumes an autonomy of self that includes freedom of thought, belief, expression, and certain intimate conduct.

Id.; see also Griswold, 381 U.S. at 485-86 ("Would we allow the police to search the sacred precincts of marital bedrooms for telltale signs of the use of contraceptives? The very idea is repulsive to the notions of privacy surrounding the marriage relationship.").

n338. Martin v. City of Struthers, 319 U.S. 141, 147 (1943).

n339. 487 U.S. 474 (1988).

n340. Id. at 484-85 (citations omitted).

n341. 397 U.S. 728 (1970).

n342. See, e.g., U.S. West, Inc. v. FCC, 182 F.3d 1224, 1235 (10th Cir. 1999) ("We have some doubts about whether this interest, as presented, rises to the level of "substantial.'").

n343. Mainstream Mktg. Servs. Inc. v. FTC, 283 F. Supp. 2d 1151, 1168 (D. Colo. 2003) (holding Do-Not-Call Registry unconstitutional under Central Hudson), rev'd, 358 F.3d 1228 (10th Cir. 2004).

n344. Mainstream Mktg. Servs., 358 F.3d at 1242.

n345. Cf. U.S. West, 182 F.3d at 1239 (holding the regulations were not narrowly tailored and thus failed the fourth prong of the Central Hudson analysis).

n346. See, e.g., Illinois ex rel. Madigan v. Telemarketing Assocs., Inc., 538 U.S. 600 (2003) (holding the First Amendment does not bar a fraud claim against telemarketers who make misleading statements about the way donations would be used); see also Telephone Consumer Protection Act of 1991, 47 U.S.C. 227 (2000) (regulating telemarketing).

n347. Cf. Schauer, supra note 95, at 176 (describing the First Amendment as an "argumentative showstopper[]"). One possible exception to this rule is child pornography, which forces even zealous First Amendment absolutists to get off the bus. For an explanation of this phenomenon, see generally Amy Adler, Inverting the First Amendment, 149 U. Pa. L. Rev. 921 (2001); Amy Adler, The Perverse Law of Child Pornography, 101 Colum. L. Rev. 209 (2001).

n348. See, e.g., Volokh, supra note 3, at 1050-51; sources cited supra notes 57-59.

n349. See sources cited supra notes 53-56.

n350. See Lochner v. New York, 198 U.S. 45 (1905) (invalidating a New York statute setting maximum hours for bakers on due process grounds). Scholars in the analogous areas of cyberlaw and intellectual property have, however, identified a resurgence of Lochner-style arguments in those areas of law. See Julie E. Cohen, Lochner in Cyberspace: The New Economic Orthodoxy of "Rights Management," 97 Mich. L. Rev. 462 (1998); Paul M. Schwartz & William Michael Treanor, Eldred and Lochner: Copyright Term Extension and Intellectual Property as Constitutional Property, 112 Yale L.J. 2331 (2003).

n351. See Barry Friedman, The History of the Countermajoritarian Difficulty, Part Three: The Lesson of

Lochner, 76 N.Y.U. L. Rev. 1383, 1392 (2001).

n352. White, supra note 8, at 241-42.

n353. Friedman, supra note 351, at 1385; see also David E. Bernstein, Lochner's Legacy's Legacy, 82 Tex. L. Rev. 1, 2-4 (2003) (collecting sources); Friedman, supra note 351 (same).

n354. See, e.g., Jack Balkin, Digital Speech and Democratic Culture: A Theory of Freedom of Expression for the Information Society, 79 N.Y.U. L. Rev. 1 (2004); Julie E. Cohen, Lochner in Cyberspace, 97 Mich. L. Rev. 462 (1998).

n355. See, e.g., Barry Cushman, Rethinking the New Deal Court (1998); White, supra note 8; Michael Les Benedict, Laissez-Faire and Liberty: A Re-Evaluation of the Meaning and Origins of Laissez-Faire Constitutionalism, 3 Law & Hist. Rev. 293 (1985); Charles W. McCurdy, The Roots of "Liberty of Contract" Reconsidered: Major Premises in the Law of Employment, 1867-1937, 1984 Y.B. Sup. Ct. Hist. Soc'y 20. For a more detailed overview of such efforts, see generally Friedman, supra note 351, at 1397-1402 (collecting sources).

n356. William M. Wiecek, The Lost World of Classical Legal Thought: Law and Ideology in America, 1886-1937, at 3 (1998).

n357. See Cushman, supra note 355, at 6-7.

n358. See White, supra note 8, at 167-70.

n359. See id. at 168-74.

n360. See id. at 3-4.

n361. See Friedman, supra note 351, at 1399-1400 (collecting sources).

n362. Cushman, supra note 355, at 3, 7; White, supra note 8, at 241-46.

n363. See Friedman, supra note 351, at 1420-28.

n364. Wiecek, supra note 356; see also William M. Wiecek, The Rise and Fall of Classical Legal Thought: Preface to the Modern Constitution, in Constitutionalism and American Culture: Writing the New Constitutional History 64, 66 (Sandra F. VanBurkleo et al. eds., 2002).

n365. Friedman, supra note 351, at 1453-56.

n366. Id. at 1386-87.

n367. Id.

n368. In only a few months after the creation of the Do-Not-Call Registry, over fifty million phone numbers were registered. When on September 23, 2003, a federal district court invalidated the Registry as lacking sufficient congressional authorization, United States Sec. v. FTC, 282 F. Supp. 2d 1285, 1290-91 (W.D. Okla. 2003) (holding that Congress had not given the FTC sufficient authorization to implement the Registry), there was an enormous public outcry. In response, Congress took the almost unprecedented step of reversing the district court by passing a statute in little more than a day. See Adam Zitter, Note, Good Laws for Junk Fax? Government Regulation of Unsolicited Solicitations, 72 Fordham L. Rev. 2767, 2767 (2004).

n369. See supra notes 31-45.

n370. See Richards, supra note 144, at 781-82. For exceptions, see White, supra note 8, and Freyer, supra note 144.

n371. See Richards, supra note 144, at 781-82.

n372. See White, supra note 8, at 128-63; G. Edward White, The First Amendment Comes of Age: The Emergence of Free Speech in Twentieth-Century America, 95 Mich. L. Rev. 299 (1996).

n373. 304 U.S. 144, 152 n.4 (1938).

n374. See Richards, supra note 144, at 900.

n375. White, supra note 372, at 309.

n376. See supra note 150 and accompanying text.

n377. 316 U.S. 52 (1942).

n378. 341 U.S. 622 (1951).

n379. Murdock v. Pennsylvania, 319 U.S. 105, 115 (1943).

n380. 425 U.S. 748 (1976).

n381. Id. at 763-64.

n382. Id. at 765.

n383. For example, Justice Rehnquist argued in dissent that:

The Court speaks of the importance in a "predominantly free enterprise economy" of intelligent and well-informed decisions as to allocation of resources. While there is again much to be said for the Court's observation as a matter of desirable public policy, there is certainly nothing in the United States Constitution which requires the Virginia Legislature to hew to the teachings of Adam Smith in its legislative decisions regulating the pharmacy profession.

Id. at 783-84 (Rehnquist, J., dissenting); see also Cent. Hudson Gas & Elec. Corp. v. Pub. Serv. Comm'n, 447 U.S. 557, 591 (1986) (Rehnquist, J., dissenting) (arguing that the Court had, "by labeling economic regulation of business conduct as a restraint on "free speech,' gone far to resurrect the discredited doctrine of cases such as Lochner").

n384. See, e.g., Thomas H. Jackson & John Calvin Jeffries, Jr., Commercial Speech: Economic Due Process and the First Amendment, 65 Va. L. Rev. 1, 40 (1979) (characterizing the case as "the revivification of economic due process in the guise of commercial speech").

n385. See Schauer, supra note 98, at 1780 (collecting sources).

n386. See id.

n387. See id. at 1777-84.

n388. See, e.g., Mark A. Lemley & Eugene Volokh, Freedom of Speech and Injunctions in Intellectual Property Cases, 48 Duke L.J. 147 (1998); Eugene Volokh, Crime-Facilitating Speech, 57 Stan. L. Rev. (forthcoming Feb. 2005); Eugene Volokh, Freedom of Speech and Intellectual Property: Some Thoughts After Eldred, 44 Liquormart, and Bartnicki, 40 Hous. L. Rev. 697 (2003); Eugene Volokh, Freedom of Speech and the

Right of Publicity, 40 Hous. L. Rev. 903 (2003); Volokh, supra note 131; Eugene Volokh, What Speech Does "Hostile Work Environment" Harassment Law Restrict?, 85 Geo. L.J. 627 (1997); Eugene Volokh & Brett McDonnell, Freedom of Speech and Independent Judgment Review in Copyright Cases, 107 Yale L.J. 2431 (1998).

n389. Perhaps recognizing this tension, the Supreme Court in the recent case Eldred v. Ashcroft rejected the assertion of public interest groups that federal copyright statutes regulate speech and thus warrant intermediate First Amendment scrutiny. Eldred v. Ashcroft, 537 U.S. 186, 218-21 (2003). Justice Ginsburg's opinion for the Court rested on a number of justifications, including the fact that copyright law includes a number of internal speech-protective mechanisms, but implicit in its treatment of the issue seems to be a judgment that heightened scrutiny would unduly handicap Congress in its formulation of information policy more generally. Id. at 218-22.

n390. See, e.g., Randy E. Barnett, Restoring the Lost Constitution: The Presumption of Liberty 253-54 (2004) (arguing for a rejection of "the pure Footnote Four approach" in favor of a constitutionalism that protects economic as well as political liberties); Walter Dellinger, The Invisibility of Economic Rights and Personal Liberty, in 2003-2004 Cato Supreme Court Review 9, 13-16 (Mark K. Moller et al. eds., 2004).

n391. Emerson, supra note 70, at 76.

n392. See supra note 285.

TAB 17

10 of 15 DOCUMENTS

Northwestern University Law Review

Spring, 2002

96 Nw. U.L. Rev. 1099

LENGTH: 35292 words

ARTICLE: Information as Contraband: THE FIRST AMENDMENT AND LIABILITY FOR TRAFFICKING IN SPEECH

NAME: Rodney A. Smolla*

BIO: * George E. Allen Professor of Law, University of Richmond School of Law.

SUMMARY:
... Yet the confusing alignment of the Justices makes the precise holding of the case far from clear, and what at first blush seemed a setback for the protection of privacy may on further review prove a backhanded victory. ... Since the parties, and their amici in briefs and in oral argument, labored prodigiously over this question, and since the concurring opinion of Justices Breyer and O'Connor explicitly stated that "intermediate scrutiny" was the Court's standard while the dissenting opinion of the Chief Justice complained mightily that strict scrutiny was in fact what the Court had employed, go figure what the Court had in mind with its studied obscurity. ... Indeed, the opinions of the five concurring and dissenting Justices would collapse on themselves if this were what they meant, for the very device used to strike the "reasonable" balance between privacy and speech those Justices would employ - the newsworthiness defense - would simultaneously tilt the balance entirely in favor of speech, by treating the now-revised law as content based, thereby upping the ante of judicial review to strict scrutiny. ... The "newsworthiness" defense contemplated by the concurring and dissenting Justices, a defense that would not itself be independently subject to strict scrutiny, serves essentially the same function as "fair use" and the "idea-expression" dichotomy in copyright law. ...

TEXT:
[*1099]

Introduction

May the government treat information as contraband, rendering illegal its mere possession or receipt? May the government impose liability for "trafficking" in information contraband, prohibiting disclosure of information others have unlawfully obtained?

These issues arise in a surprising array of different circumstances, yet American law has never quite fully come to grips with them. Consider a few of the many permutations: To protect privacy, the government makes it illegal to intercept electronic communications, such as conversations on a cellular telephone. The government may certainly punish the eavesdropper; but if the eavesdropper records the conversation and turns the tape over to a broadcast journalist, may the government also punish the journalist for broadcasting the purloined conversation? To safeguard national security, the government classifies information, declaring it secret. The government may punish its own employees for leaking classified material to outsiders; but may it also punish those outsiders - The Washington Post, perhaps, or CNN - for further disseminating the classified material? To protect intellectual property, the government forbids the unauthorized copying of copyrighted works, exempting from the prohibition a defined category of "fair

uses"; but may the government also punish those who traffic in information designed to facilitate the illegal copying of protected material? To protect the citizenry from violent crime, the government may punish murder, including those who traffic in it for meretricious gain, such as professional assassins. But may the government also punish those who assist in the training of those professional assassins, trafficking in information calculated to educate would-be killers in the instruments and techniques of murder for hire?

Fertile imaginations will undoubtedly conjure any number of additional scenarios, but the examples above illustrate common repeating patterns. Laws created (or future laws imagined) for the purpose of treating information as contraband generally fall into four categories: (1) laws designed **[*1100]** to protect individual privacy, (2) laws designed to protect official secrets, (3) laws designed to protect intellectual property, and (4) laws designed to deter facilitation of criminal or tortious conduct. The categories are not mutually exclusive - a given law may partake of more than one of these purposes - and the list is not necessarily exhaustive - there are sure to be other examples, present and future - but this collection does seem to capture the principal contemporary prototypes, and is clearly sufficient to provide grist for analysis.

Treating information as contraband poses serious and vexing First Amendment questions. Surprisingly, we have done little as a society to resolve them. The questions have been frequently noted and avoided by courts, but only rarely engaged head-on. For its part, the Supreme Court has been making neat and passing mention of these First Amendment questions for nearly three decades. Not until the summer of 2001, however, in Bartnicki v. Vopper, n1 did the Court pass judgment on any of them. Bartnicki, a case much-watched and much-awaited, must now be much-deciphered. In Bartnicki, the Court held that federal and state statutes prohibiting the disclosure of information obtained through illegal interception of cellular phone messages were unconstitutional as applied to certain media and nonmedia defendants who received and disclosed to others tape recordings of the intercepted messages from anonymous sources. Yet the confusing alignment of the Justices makes the precise holding of the case far from clear, and what at first blush seemed a setback for the protection of privacy may on further review prove a backhanded victory.

This Article ranges widely, exploring the treatment of information as contraband in arenas as diverse as privacy, official secrets, intellectual property, defamation, and liability for facilitating criminal or tortious conduct. The discussion is top-heavy with privacy contraband, because that is the subject of the holding in Bartnicki, the Supreme Court's latest and most significant word. But Bartnicki will not be the last word - on privacy contraband, or any of the other myriad contraband laws society may adopt to deter trafficking in socially destructive behavior - and this Article explores the tensions in policy and law that will continue to animate debate over the propriety and constitutionality of making it illegal to traffic in proscribed categories of speech.

I. Privacy Contraband

A. Eavesdropping Laws and Electric Contraband

In 1968, Congress passed a statute, Title III of the Omnibus Crime Control and Safe Streets Act of 1968, n2 to prohibit electronic eavesdropping. The law was amended in 1986 to bring new technologies, including cellular **[*1101]** phones, within its ambit. The law prohibits not only the interception of electronic communications, but also the subsequent disclosure or use of the contents of the communication by any person knowing or having reason to know that the communication was obtained illegally. n3 In addition to criminal penalties, Title III provides for a civil action against any person who intentionally violates the Act. n4 More than forty states, n5 including Pennsylvania, n6 (where Bartnicki arose) have enacted laws following the **[*1102]** federal model.

Most of us are just now slowly learning to take care with our words on cell phones and e-mail, for others may be listening or reading. n7 But our prescient Congress, back in the quaint pre-Internet and pre-cell-phone days of 1968, had already identified the specter of a grievous threat to privacy in new communications technologies, describing in the legislative history the "widespread use and abuse of electronic surveillance techniques." n8 A Senate Report noted that the "privacy of communication is seriously jeopardized," n9 and articulated the fear that "every spoken word relating to

each man's personal, marital, religious, political, or commercial concerns can be intercepted by an unseen auditor and turned against the speaker to the auditor's advantage." n10 By the time the process of amending Title III began in 1984, with the aim of expanding it to take in a wider range of new technologies, Congress's concern for protecting the privacy of electronic communications had been significantly amplified. n11 Yet even the Orwellian year 1984 seems primitive from our new millennium perspective.

Perhaps our politicians acted early and aggressively on this issue because they themselves have privacy interests at stake. Whatever may account for its perspicacity, Congress clearly understood that new communications technologies would often supplement, if not largely supplant, many traditional forms of communication such as first-class mail or the traditional hard-wired land phone, forms of communication that historically promised a reasonably strong degree of privacy protection. n12 Congress **[*1103]** plainly thought it was important to attempt to secure some rough measure of equivalent privacy for these new modes of communication, and for new forms that would undoubtedly develop in the future, given our modern culture's ever-accelerating arc of invention. n13

B. A Society of Scanners

There's a whole lot a scannin' goin' on. Federal law does not make it a crime for you to secretly tape a conversation if you are a party to it. n14 However, it is a crime if you are not.

A scanner is simply a machine, the kind of thing you can buy at Radio Shack. You use this machine to eavesdrop. In 1993, Congress made it illegal to market the scanners themselves, at least the kind that could be used to intercept cell phone calls. n15 But there is a quicksilver ingenuity in techno-snoop culture, and the law is easily evaded. Scanners that do not come built with the capacity to capture cellular transmissions are easily converted into scanners that do. n16 People scan for motives meretricious and malicious. People scan for sport. What we know is that they scan a lot, and that there are a lot of scanners. Scanners of the sort used to intercept cellular telephone calls are ubiquitous, with over ten million such devices in circulation. n17

There is indeed a whole lot a scannin' goin' on. People surreptitiously intercept, record, and disclose the usual suspects for the usual reasons, in the perpetual parade of human perfidy. Popular motivations are love, sex, drugs, crime, politics, business, and employment. And if we reflect, we quickly see that none of us is perfect and that all of us are potential victims. **[*1104]** Who among us does not sometime, somewhere, have something they would prefer to keep to themselves?

As one would expect, reported cases are awash in detritus of domestic dysfunction - disputes arising from divorce, n18 child custody, n19 child-parent suits, n20 and other conflicts of the heart. n21 Political hijinks are another popular motive. (As previously noted, this may explain why our political leaders are so sensitized to spying. n22) Business disputes, including industrial espionage, n23 **[*1105]** and labor and employment disputes are also common motivations. n24 Police and government investigations also trigger scanning incidents in every imaginable configuration of perpetrator, n25 investigator, n26 and officious intermeddler. n27 The examples are not exhaustive.

C. Techno-Paparazzi

There are many ingenious ways to invade privacy, of course, other than the interception of cell phone transmissions. One of the newest trends in privacy-protecting legislation (enacted and proposed) incorporates a concept known as "constructive trespass," in which it is deemed an invasion of privacy to use technology to intrude into areas of seclusion that would, in **[*1106]** the absence of the technical innovation, have required a more conventional physical invasion. California has enacted such legislation. n28 The California law forbids invasions of privacy for the purposes of capturing images about a person engaging in "personal or familial activity" when the invasion occurs in a manner that is offensive to a reasonable person, if the invasion is done for a commercial purpose. n29 Liability is imposed for "constructive invasions of privacy" by banning intrusions through the use of technical means that enable intrusions not otherwise possible without a trespass. n30 The law is calibrated both in terms of the space invaded and the nature of the

activity observed; not every invasion is covered, but only those into "personal and familial" activities, which the law defines as including crime victims, the "intimate details of the plaintiff's personal life, interactions with the plaintiff's family or significant others, or other aspects of plaintiff's private affairs or concerns." n31 Anticipating an issue that would ultimately become pivotal in Bartnicki, the California law specifically excludes from its coverage private activity that is illegal. n32 Only invasions effectuated **[*1107]** for a "commercial purpose" - defined as invasions perpetrated with the expectation of sale, financial gain, or consideration - are prohibited. n33 The law also holds liable any person who directs, induces, or solicits the invasion of privacy, whether or not there is an employer-employee relationship. n34 The statute does not, however, go so far as to create true "privacy contraband," in the same sense that Title III does for intercepted electronic communications - mere publication of material obtained in violation of the law does not itself constitute a violation. n35 In the United States Congress, several bills have been proposed that follow the California lead. n36 Senators Orrin Hatch and Dianne Feinstein cosponsored a bill in 1998 forbidding certain privacy invasions for commercial purposes; the bill appeared largely targeted at paparazzi tactics and, like the California statute, contained prohibitions that reach "constructive" privacy invasions. n37

D. Comparing Common-Law Privacy Actions

It is illuminating to compare the statutory antitrafficking provisions of electronic eavesdropping statutes with common-law causes of action for invasion of privacy. n38 The tort of "intrusion," as it is classically defined, has **[*1108]** not been traditionally understood as creating "privacy contraband" in the same sense as the eavesdropping laws. The intrusion tort forbids intentional invasions of the solitude or seclusion of another that would be highly offensive to a reasonable person. n39 A strong case can be made that intentional interceptions of cell phone communications through a scanner of the sort prohibited by Title III and similar state laws would also in most instances satisfy the elements of intrusion. But the common-law tort of intrusion, unlike the electronic eavesdropping statutes, does not turn the fruits of the intrusion into instant contraband, making those who come into possession of it "downstream" liable for subsequent disclosure of the information. To the contrary, if a wrongdoer breaks into the private spaces of the plaintiff to capture private information, and then turns over the pilfered information to a journalist, the traditional rule is that the journalist may publish the material, even when knowing it was obtained illegally. n40

An entirely different common-law tort, however, known as "publication of private facts," does create a form of privacy contraband. This tort permits recovery for the damages caused by public disclosure of a private fact in circumstances that would be offensive and objectionable to a reasonable person, when the revelation is not newsworthy. n41 The "contraband" in the private facts tort is not defined by how the information was obtained but **[*1109]** on the content of the information itself. Courts ask whether the information is genuinely "private," and whether, even if "private," it is nonetheless newsworthy. Information that is private and not newsworthy may not be disseminated, even if it was obtained "legally" by the media through no wrongdoing by the media themselves or, for that matter, through no wrongdoing by anyone.

The contraband aspect of the private facts tort is at once broader and narrower than eavesdropping statutes. It is broader in the sense that contraband status may exist even though the information was not obtained through some independently tortious or criminal activity. It is narrower in that the material must pass through two subject-matter filters before a claim becomes actionable - one filter to determine whether the material is private, and another to determine whether it is newsworthy.

To date, the private facts tort has had a less than meteoric career. Its problem is not that it lacks a solid definition to the concept of "private fact." That part has been easy - judges and juries appear to face no great conceptual difficulty identifying those aspects of life that are sufficiently intimate or personal to qualify as nobody else's business. Matters relating to sexuality, love, physical and mental health, family relationships, intense religious and political convictions, and personal finances are among the topics regarded as private. n42 The law of torts, applying its usual earthy touchstones of the reasonable person and community standards, seems perfectly well equipped to give these concepts adequate definition. n43

The rub has been with the concept of "newsworthiness." n44 It bears an enormous load, and courts are understandably ambivalent about presuming to second-guess journalistic judgment by holding that a fact which a journalist has already adjudged sufficiently newsworthy was, on further review of the play, wrongly classified. n45 Many in society are offended by much of **[*1110]** what is reported in the press, perceiving it as sleazy, sensational, and salacious. We are in a period of deep cultural funk over the politics of personal destruction. Yet, the First Amendment must be grounded in rules firmer than subjective taste, and courts usually realize that the mere fact that a revelation is offensive to many, or most, in the community does not mean it is not newsworthy. n46 We may not like the tabloidization of American culture, but as long as the First Amendment remains a salient part of the conversation, there are limits to what the law can do about it. Newsworthiness is thus the gatekeeper, and the gate to a plaintiff's recovery is often shut. n47

The issue here runs deep. If the First Amendment is understood as offended in some absolute sense by any courtroom second-guessing of a journalist's news judgment, then the First Amendment entirely swallows the private facts tort. n48 The whole notion of a tort of publication of private facts with a newsworthiness defense built-in is unintelligible unless we permit judges and juries to make the determination, as "objectively" as they can, of what is and is not "news" - or precisely, news worthy of the First Amendment.

Those courts that have struggled with this question most seriously over the years appear to recognize that the existence of the tort is only possible if juries and judges determine newsworthiness through some balancing process that includes an assessment of community norms. In California, for example, the newsworthiness test involves a balancing of the social value in the facts published, the depth of the article's intrusion into private affairs, and the extent to which the victim of the invasion voluntarily assumed a position of fame or notoriety. n49 Courts apply this test with a considerable degree **[*1111]** of nuance; material deemed of little social value in which the degree of intrusiveness into private spheres is high, may thus be deemed nonnewsworthy even though it involves a public figure. A federal district court held, for example, that Bret Michaels, lead singer of the rock band "Poison," and Pamela Anderson Lee, a well-known television and film star, had a probability of success in defeating a newsworthiness privilege in a case that involved the distribution of video footage showing them engaged in sexual activity, issuing a preliminary injunction against its release. n50

Tellingly, judicial attempts to define newsworthiness bear a striking resemblance to judicial efforts to define obscenity, a concept the Supreme Court has directly tied to community mores. n51 A jury in an obscenity case must determine such things as whether material is patently offensive, applying **[*1112]** community standards, or whether a work has serious redeeming social value. There is arguably little difference between these determinations and a decision about whether the public revelation of an ostensibly private fact is or is not newsworthy. n52

If the First Amendment means that the media may never be held liable for publishing true facts that were not obtained through any direct wrongdoing by the media themselves - if a publication of private facts tort can, in effect, never exist unless coupled with a direct violation of privacy by the media, akin to an action for illegal eavesdropping, constructive trespass, or intrusion - then the publication of private facts tort simply cannot exist in our constitutional system.

Against this backdrop, the stakes being wagered in the Supreme Court's decision in Bartnicki were prodigious, expanding far beyond the issues posed by Title III and its state-law counterparts. The whole notion of privacy contraband was at play in Bartnicki, and depending on what the Court ruled, and how broadly or narrowly it cast its ruling, protection of privacy in the United States stood to be significantly reinvigorated - or significantly reduced.

E. A Critical (and Highly Annotated) Reading of Bartnicki v. Vopper

1. Bartnicki's Facts: Blowin' Up Porches and Getting Dose Guys.

- Gloria Bartnicki was a principal labor negotiator for a teachers' union, the Pennsylvania State Education Association.

Anthony Kane, a high school teacher at Wyoming Valley West High School, was president of the union. In May of 1993, Bartnicki and Kane had a telephone conversation concerning the ongoing labor negotiations with a local school board. Kane was speaking from a land phone at his house. Bartnicki was talking from her car, using her cellular phone. Strategies and tactics were discussed, including the possibility of a teacher strike. The talk was candid, and included some blunt down-and-dirty characterizations of their opponents in the labor controversy, at times getting personal. One of the school district's representatives was described as "too nice," another as a "nitwit," and still others as "rabble rousers." Among the opposition tactics that raised the ire of Bartnicki and Kane was the proclivity, in their view, of the school district to negotiate through the newspaper, attempting to pressure the teachers' union by leaks to the press. The papers had reported that the school district was **[*1113]** not going to agree to anything more than a pay raise of three percent. As they discussed this position, Kane stated: "If they're not gonna move for three percent, we're gonna have to go to their, their homes ... to blow off their front porches, we'll have to do some work on some of those guys." n53

An unknown person intercepted the conversation, presumably using a scanner that picked up the cell phone transmissions, recording it on a cassette tape. This unknown person placed the tape in the mail box of the Jack Yocum, president of a local taxpayer's group that was opposed to the teachers' union and its bargaining positions. Yocum listened to the recording, recognized the voices of Bartnicki and Kane, and took the tape to Frederick Vopper, a local radio station talk show host. n54 Vopper received the tape in the spring of 1993, but waited until late September to broadcast it, which he did a number of times. At first Vopper broadcast a part of the tape that revealed Bartnicki's phone numbers. She began to receive menacing calls, and was forced to change her numbers. The tape was later warped so that the numbers would be indistinguishable when it was played on the air. Yocum, who first received the tape, and Vopper, who played it on the radio, both realized it had been intercepted from a cell phone, and that a scanner had probably been used to make the intercept. Other media outlets, including a newspaper in Wilkes-Barre, also received copies of the tape, but no other broadcaster or publisher played the tape or disclosed its contents until the material on the tape was broadcast by Vopper. Once Vopper broke the story, however, secondary coverage of the events, including the contents of the tape, appeared in other media outlets. Invoking a federal statute and a very similar Pennsylvania law, Bartnicki and Kane sued Yocum, Vopper, and the radio stations that carried Vopper's show, for having used and disclosed the tape of their intercepted telephone conversation.

2.The Supreme Court Score Card: When a Majority Is Really a Plurality.

- The Supreme Court asserted review in Bartnicki following a decision by the United States Court of Appeals for the Third Circuit holding the federal and state statutes unconstitutional. n55 Justice Stevens wrote the opinion of the Court, which was nominally joined by Justices Kennedy, Souter, Ginsburg, Breyer, and O'Connor. However, these appearances are deceiving. Although decided by a six-to-three majority, two of the Justices in the majority - Breyer and O'Connor - concurre d in an opinion written by Justice Breyer that appeared to dramatically trim the reach and rationale of the majority opinion. The holding in Bartnicki, that broadcast of the intercepted cell phone conversation was protected by the First Amendment, was thus narrowed in two ways: first, by the numerous explicit limitations placed on the reach of the decision in Justice Stevens's opinion for the **[*1114]** Court, and second, by the substantial and important additional limitations articulated in Justice Breyer's concurring opinion. Indeed, the nominal "opinion of the Court" in Bartnicki may well not be that at all. Justice Stevens's opinion is more aptly described as a four-Justice plurality decision, a decision that is quite sharply and dramatically constrained by the limiting language in the Breyer and O'Connor concurrence.

This has happened before in mass media law and there is some irony in its repetition. In Branzburg v. Hayes, n56 the Supreme Court appeared to reject, by a five-to-four vote, the notion that there was any "reporter's privilege" emanating from the First Amendment protecting journalists from disclosure of confidential sources. The opinion of the Court, written by Chief Justice Burger for what appeared to be five Justices, was brusque and unequivocal, squarely repudiating the recognition of any such privilege. n57 In a short three-paragraph concurring opinion, however, Justice Powell wrote separately, in his words, to "add this brief statement to emphasize what seems to me to be the limited nature of the Court's holding." n58 He went on to suggest that it might be appropriate to balance the competing interests

at stake on a case-by-case basis. n59

[*1115] Notwithstanding the apparently resounding defeat in Branzburg for the press, many lower courts, relying on Justice Powell's concurring opinion, held that the First Amendment did provide a conditional reporter's privilege of some kind. n60 Not all lower courts have been persuaded by this movement, and the question of whether the First Amendment does or does not provide a "reporter's privilege" of some kind remains a matter of debate, n61 fueled in part by ambivalent signals from the Supreme Court itself. n62 The **[*1116]** important point of the story is that a short concurring opinion by a Justice who actually joined the opinion of the Court in Branzburg in effect superseded the majority opinion and became the prevailing law of the land.

If to live by the concurrence is to die by the concurrence, the press's victory in Bartnicki could over time prove every bit as pyrrhic as its defeat in Branzburg. The concurring opinion of Justices Breyer and O'Connor in Bartnicki may well be used to spin a constitutional doctrine that would empower the government to forbid trafficking in privacy contraband, despite a majority opinion that on its surface seemed to deny it. Indeed, the structure, substance, and tone of Justice Breyer's opinion in Bartnicki were remarkably similar to that of Justice Powell in Branzburg. Justice Breyer began with an echo of Powell's opening line, stating "I join the Court's opinion because I agree with its "narrow' holding, ... limited to the special circumstances present here." n63 As described in detail in the following critical reading of Bartnicki, what Justices Breyer and O'Connor appeared to mean by these "special circumstances" has enormously important implications for the future of attempts to protect privacy through recognition of privacy contraband. n64

3.The Court's Narrowing Assumptions. - The opinion of Justice Stevens began its substantive analysis by reciting the factual assumptions that it accepted in framing the constitutional question before the Court. First, the Court assumed that the interception of the phone conversation was intentional and unlawful, even though the actual perpetrator was unknown, and that, at a minimum, Yocum and the media outlets that disclosed the contents of the conversation "had reason to know" the original interception was unlawful. n65 This meant that Yocum and the media defendants had violated the federal and Pennsylvania disclosure statutes and could be held liable under those laws if they were constitutionally valid.

The Court also accepted, as if it were a similarly mundane "fact," the supposition that the access of the defendants "to the information on the tapes was obtained lawfully, even though the information itself was intercepted unlawfully by someone else." n66 Significantly, neither the three dissenters n67 nor Justices Breyer and O'Connor n68 were quite so sanguine about this cheery assumption and the tacit judgments of law and policy embedded in it. Justice Stevens's opinion also assumed that the subject matter of the **[*1117]** intercepted conversation was a matter of public concern. The announced logic for this judgment was that the statements would clearly have been "newsworthy" had they been made in an open public arena, such as in the process of collective bargaining. Since the statements would have been newsworthy if made openly, Justice Stevens explained, they were newsworthy when made in a private conversation. n69

The Court in Bartnicki made abundantly clear that it was not answering the ultimate question of whether the media may ever be held liable for publishing truthful information lawfully obtained, but was rather addressing what it described as "a narrower version of that still-open question," n70 which it put as: ""Where the punished publisher of information has obtained the information in question in a manner lawful in itself but from a source who has obtained it unlawfully, may the government punish the ensuing publication of that information based on the defect in a chain?"' n71

These various efforts to narrow the reach of the Court's holding in Bartnicki have immense significance, particularly when coupled with the spin placed on them by Justices O'Connor and Breyer. n72 But there was arguably more to it than mere spin. Philosophically, the bridging opinion of Justices Breyer and O'Connor was more simpatico with the values expressed by the Chief Justice and Justices Scalia and Thomas in dissent than it was with the opinion for the Court authored by Justice Stevens. Indeed, Justice Stevens's opinion was plagued throughout by a disturbingly hurried quality, with many of the most critical issues examined on the fly. The Court often failed to engage at any complex level the most significant questions, and when it did engage, its pronouncements, even on issues so basic as the

standard of review it was applying, appeared deliberately obscured. n73

4.Content, Viewpoint, and Laws of General Applicability.

- At the threshold of most of the important modern First Amendment cases, one finds the Supreme Court engaged in an open (if not always easy) inquiry into the appropriate "standard of review" or doctrinal test to be applied. n74 **[*1118]** In Bartnicki, at least three different doctrinal standards were plausible nominees. One might treat Title III as a "neutral law of general applicability" not regulating speech at all, and thus triggering no heightened First Amendment review of any kind. n75 As such, it would be subject to mere "rational basis" review, and almost certainly constitutional. n76 At the opposite extreme, one might treat Title III as a content-based regulation of speech, subjecting it to the rigors of "strict scrutiny" review. n77 Finally, one might treat Title III as content neutral, but as nonetheless exacting an incidental "impact" on expression, and opt for the "intermediate scrutiny" standard usually applied in such circumstances. n78

Astonishingly, at no point in Justice Stevens's opinion does the Court come right out and say what standard of review or doctrinal test it is applying to the laws before it. Since the parties, and their amici in briefs and in oral argument, labored prodigiously over this question, and since the concurring opinion of Justices Breyer and O'Connor explicitly stated that "intermediate scrutiny" was the Court's standard n79 while the dissenting opinion of the Chief Justice complained mightily that strict scrutiny was in fact what the Court had employed, n80 go figure what the Court had in mind with its studied obscurity. There were plenty of proofreaders, so it wasn't as if the Justices just, uh, forgot. Quite to the contrary, there was a strange ambiguity to Justice Stevens's opinion on this point, a too-casual-to-really-becasual smattering of little half-hints that could be taken either way. At the part of the opinion that came closest to confessing some actual doctrinal standard, the Court stated that "unusual cases fall far short of a showing that there is a "need of the highest order' for a rule supplementing the traditional means of deterring antisocial conduct." n81 The phrase "highest order" came from a line of cases that was traditionally understood as a doctrinal **[*1119]** synonym for "compelling governmental interest," one of the prongs of strict scrutiny. n82 This was followed, however, by a quote from a case applying intermediate scrutiny, n83 and a footnote citation to the commercial speech standard, another doctrinal variant of intermediate scrutiny. n84 Finally, the Court at one point in its opinion conceded that protecting privacy in communication is an "important interest," n85 a phrasing that would seem to denote application of intermediate scrutiny. The essential point is that even taking the opinion of the Court in Bartnicki on its own terms (such as they are), again and again one is left with the impression that there is at once more, and less, to the opinion of the Court than meets the eye.

Having said all this, however, it appears the soundest understanding of Bartnicki is that it applied intermediate scrutiny. Indeed, only intermediate scrutiny received the explicit endorsement of five Justices - the two concurring votes of Justices Breyer and O'Connor, n86 and the three dissenting votes of Chief Justice Rehnquist and Justices Scalia and Thomas. n87 More significantly, only intermediate scrutiny makes sense.

Antitrafficking laws of the sort at issue in Bartnicki really cannot properly be understood as "neutral laws of general applicability," at least as that term of art has been classically reserved in First Amendment jurisprudence for laws that actually do not regulate speech at all. Our jurisprudence attempts to differentiate between "neutral laws of general applicability" and laws that are "content neutral." Although both phrases include the word "neutral," one is more neutral than the other. The term of art "neutral laws of general applicability" is most properly reserved for laws that are best understood as not being "speech laws" in any genuine sense. n88 They do not **[*1120]** regulate speech, but rather regulate some other aspect of human behavior. n89 Behavior may involve the use of language, evidence of a party's expressive activity may be introduced to prove the elements of the case, and the application of the law may in some circumstances implicate speech or the process of newsgathering, but these intersections with speech are regarded as mere happenstance. n90 The Supreme Court's well-known decision in Cohen v. Cowles Media Co., n91 for example, held that the First Amendment did not prevent Minnesota from using its law of contracts and promissory estoppel in a suit brought by a source for breach of a promise of confidentiality made to the source by a journalist. In Cohen, there were numerous intersections with expressive activity. The promise made by the journalist to Dan Cohen to keep his

identity secret involved the use of language. The breach of that promise by the journalist and the newspaper was effectuated entirely through expressive activity - publication of Cohen's name in the newspaper. The newspaper printed the truth, Cohen's identity, and his identity was entirely newsworthy. The newspaper printed Cohen's name because in the exercise of its editorial judgment it determined that Cohen, a political operative, had tried to smear an opponent. Yet despite all of this, the Court refused to apply any heightened First Amendment standard to Cohen's promissory estoppel claim, stating that "generally applicable laws do not offend the First Amendment simply because their enforcement against the press has incidental effects on its ability to gather and report the news." n92

To be sure, a law that prohibits knowingly trafficking in stolen "goods" would certainly be understood as a law of general applicability and not a law governing speech. The stolen "goods" might well be expressive - they might be books, tapes, compact disks, or paintings - and any law forbidding trafficking in stolen goods would, as applied to such communicative physical objects, inevitably impact on expression. Any attempt to invoke the First Amendment as a shield from liability from trafficking in stolen goods that happen to be communicative, however, would be patently vacuous. Following the learning of Cohen, n93 courts would undoubtedly and correctly perceive such cases as controlled by the principle that generally applicable **[*1121]** laws do not offend the First Amendment simply because their enforcement against the press has incidental effects on its ability to gather and report the news.

A restriction on the disclosure of the content of the information-bearing goods, however, does appear different. The media defendants in Bartnicki argued that the difference was immense - that it rendered the law entirely content based, and thus subject to strict scrutiny. In assessing the persuasiveness of this argument, it is important to step back and look at the architecture of current First Amendment doctrine with a wide-angle lens, taking into account three related but nevertheless distinct notions: viewpoint discrimination, content discrimination, and a line of cases usually seen as freestanding, creating a presumptive right to publish truthful material lawfully obtained.

Viewpoint discrimination and content discrimination ought not be confused. Those who defended Title III in Bartnicki, including the Solicitor General, argued that because Title III was not viewpoint based, it automatically qualified for either intermediate scrutiny or rational basis review. n94 But viewpoint neutrality should be understood as a necessary condition to qualify for intermediate scrutiny, not a sufficient one. It is true that in many of its intermediate scrutiny First Amendment decisions, the Supreme Court had observed that the laws in question were not hostile to any specific message. n95 It would be a mistake, however, to garner from these jurisprudential sound bites the principle that intermediate scrutiny is available any time the government regulation appears free of any direct motive to censor on the basis of viewpoint. For this would conflate viewpoint discrimination and content discrimination, making the larger concept of content discrimination doctrinally superfluous. Under this rendition, content discrimination that is viewpoint-neutral - that is, content discrimination untainted by any invidious animus against particular messages - would be subject to less demanding intermediate scrutiny. This has not been the law, and it should not become the law. n96 Viewpoint discrimination, at its worst, involves deliberate suppression of particular views, n97 the heavy-handed brand of censorship **[*1122]** that is tantamount to thought control. n98 While all laws that discriminate on the basis of viewpoint automatically discriminate on the basis of content, not all laws that discriminate on the basis of content go so far as to single out disfavored viewpoints. Whereas viewpoint discrimination is almost per se unconstitutional, the usual default test for content-based discrimination is the highly demanding, but not absolute, strict scrutiny standard. n99 There are powerful reasons why First Amendment jurisprudence ought to be highly skeptical of content-based regulation of speech even if it appears that the particular regulation does not have its genesis in the kind of tyrannical censorial motive we classically associate with Big Brother and thought control. Evil need not be fully realized to be fully fearful. It is not that content-based regulation of speech is inherently despotic, but that it inherently lends itself to despotism, which justifies subjecting such regulation to the acid baths of strict scrutiny. n100

Prohibitions on trafficking in illegally intercepted electronic communications do not partake of this most pernicious form of viewpoint discrimination, for they apply without regard to the ideas or views expressed in the intercepted message without regard to the ideas or views of the interceptor, and without regard to the ideas or views of the person who subsequently disseminates the information. Significantly, all nine Supreme Court Justices in Bartnicki seemed to agree that nothing in Title III remotely smacked of such viewpoint-based censorship.

A much harder question, however, is determining whether Title III should be treated as content neutral. Because the coverage of Title III is triggered by the source of the speech and not its content, at first blush it seems to be "justified without reference to the content of the regulated speech." n101 Yet the First Amendment policies that bear on the question of whether to treat laws such as Title III as content neutral or content based are **[*1123]** complex. Even if the law is not content-based in the normal sense, the widespread repugnance in our society for trafficking in such privacy contraband is at least to some degree bound up in repugnance for the open airing of the content of what was intercepted. n102 The notion that private conversations are "nobody else's business" is a notion encompassing both procedure and substance, a notion that expresses contempt for the act of interception and contempt for the spreading of what was intercepted. The second half of that contempt must at least to some degree reflect something in the nature of a content-based judgment about the speech. If nothing else, the distinction between content-neutral and content-based regulation here is significantly blurred. n103

The best way to bring clarity to this blurring is to treat Title III as not sufficiently content based to justify strict scrutiny, but as having sufficient impact on speech to justify more than mere rational basis review. This is precisely what intermediate scrutiny was designed for, and it is the best judgment of what Justice Stevens and the Court intended to apply, though the explanatory language the Court used was less then crystalline. The Court's opinion first appeared to concede that the law was content neutral, actually describing it as a "content-neutral law of general applicability," n104 emphasizing that the law centered not on the subject matter of the communication but the source. n105 Apparently worried that this might invite mere **[*1124]** rational basis review, however, the Court qualified this concession, going on to treat the law as raising First Amendment concerns greater than those posed by the typical neutral law of general applicability, because the law could be "fairly characterized as a regulation of pure speech," n106 and because the law that penalized disclosure of this "pure speech" reached "truthful" information that had been "lawfully obtained." n107

In justifying this assessment, Justice Stevens sought first to distinguish between penalizing the disclosure of the contents of intercepted communications, and penalizing the mere use of those contents. A subsequent use prohibition, Justice Stevens felt constrained to concede, would not be a penalty imposed on pure speech, but rather a penalty imposed on conduct, though that conduct might involve expression as an incidental component. Justice Stevens thus noted a catalogue of such "conduct uses" of intercepted information that would not normally be thought of as pure speech, including a company's use of an illegally intercepted communication about a business rival to create a competing product, an investor's use of an illegally intercepted communication in trading in securities, a union's use of an illegally intercepted communication about management - or management's use of a similar communication about a union - to prepare a strategy for contract negotiations, a supervisor's use of information in an illegally recorded conversation to discipline a subordinate, or a blackmailer's use of an illegally intercepted communication for the purposes of extortion. n108 Justice Stevens conceded that Yocum's mere delivery of the tape to the media defendants was arguably only conduct, but he reasoned that this type of conduct, the purpose of which was to deliver communication for further dissemination, is so intertwined with the disclosure itself as to constitute pure speech, in much the same way that delivery of a pamphlet or handbill has always been understood to be speech. n109

This analysis was not wrong, it was simply opaque. As previously explained, a true neutral law of general applicability actually is not a "speech **[*1125]** law" at all, and when it happens to impact on speech, that impact is entirely coincidental. n110 Restrictions on the use of illegally intercepted communications, for example, fall into this category. n111 The antidisclosure provisions are different, however, because a prohibition on disclosure is by hypothesis a prohibition on communication. Title III's antidisclosure provision thus was a speech law, though not viewpoint based or content based. As such, the intermediate scrutiny standard used for such problems as "time, place, or manner" regulation of speech, or its close cousin, the standard in the well-known draft card burning decision, United States v. O'Brien, n112 is appropriate. Under the O'Brien intermediate scrutiny standard, laws will be sustained if they further "an important or substantial governmental interest; if the governmental interest is unrelated to the suppression of free expression; and if the incidental restriction on alleged First Amendment freedoms is no greater than is essential to the furtherance of that interest." n113 The Supreme Court has made clear that the intermediate scrutiny standard does not require the least speech-restrictive means of advancing the government's interests. "Rather, the requirement of

narrow tailoring is satisfied "so long as the ... regulation promotes a substantial government interest that would be achieved less effectively absent the regulation.'" n114 Yet at the same time, the intermediate scrutiny is by no means a free pass to regulate with impunity.

We deal here with more than verbiage. However artificial and contrived legal formulations may on some levels be, they are the tools of the discipline. It may be easy to caricature the levels of review as empty words, but to the hundreds of lower courts that must interpret and apply Bartnicki in the future, the matter will be neither academic nor amusing. There is a palpable difference in outcomes between cases tried under the strict scrutiny standard, in which the presumption against sustaining the law is heavy, and cases tried under intermediate scrutiny, in which each side tends to have a good fighting chance. n115

[*1126] In sum, despite the obscurity of the Court's opinion on this point, and the angry protests of the dissenters notwithstanding, the best construction (or reconstruction) of the standard applied in the majority opinion in Bartnicki is that it was intermediate scrutiny. Moreover, given the insistence of concurring Justices Breyer and O'Connor n116 and the three dissenters n117 that no more than this was called for, intermediate scrutiny must be understood as the holding of the Court.

5.Liability for Publishing Truth and the Problem of Conflicting Rights. - The majority opinion's difficulty in coming out forthrightly to announce that intermediate scrutiny was the appropriate standard in Bartnicki may well have arisen from the tension the Justices felt between the line of analysis that seemed to dictate intermediate scrutiny (the line explained in the section above n118) and another line of First Amendment cases, nearly three decades old, in which the Supreme Court had repeatedly stated that the First Amendment provides a high degree of protection for the publication of truthful information, n119 often emphasizing the link of such speech to **[*1127]** the democratic process. n120 (This line of precedent is often referred to in shorthand as the Daily Mail line of cases. n121) Several Justices in Bartnicki never seemed quite sure how to reconcile these two strains of free speech law.

The truism that truth is presumptively protected under the First Amendment is, like most truisms, true only as far as it goes. The "right to print the truth" cases presented a formidable analytic problem for those seeking to justify Title III, but they were by no means self-evidently invincible. First, the Daily Mail principle clearly did not apply all the time. At times, indeed, it was entirely ignored. If the First Amendment were understood to create a presumptive right to publish anything that might be deemed "true," legal recourse for a vast array of injuries effectuated through the revelation of truthful material would be eviscerated, from the revelation of trade secrets to disclosure of information that one is contractually bound to keep confidential. n122

[*1128] Second, prior to Bartnicki, the Court had always trimmed its holdings protecting the dissemination of truthful information with the caveat that such information be "lawfully obtained." n123 But the prior cases did not explain what was meant by this phrase. n124 Two plausible and very different meanings presented themselves. At minimum, of course, the phrase was clearly intended to mean that the media itself had not engaged in any affirmative lawbreaking, that it had not hacked into the computer or broken into the file cabinet. In Branzburg v. Hayes, n125 the Supreme Court sternly admonished that it "would be frivolous to assert" that "the First Amendment, in the interest of securing news or otherwise, confers a license on either the reporter or his news sources to violate valid criminal laws." n126 Newsworthy information might often be generated through criminal misconduct, and newsworthiness alone cannot confer immunity, for "although stealing documents or private wiretapping could provide newsworthy information, neither reporter nor source is immune from conviction for such conduct, whatever the impact on the flow of news." n127

If the minimum meaning of "lawfully obtained" was obvious, however, the outer limits were not. The phrase could have meant more. At least when the government has passed specific legislation making downstream **[*1129]** disclosure of the information also criminal, it would not stretch ordinary understandings of language to treat such information as not being "lawfully obtained," in exactly the same way that we do not treat the knowing receipt of stolen goods as "lawfully obtained." The Court in The Florida Star v. B.J.F., n128 in striking down a judgment against the

media for publishing the name of a rape victim inadvertently disclosed by the police themselves, explicitly reserved judgment on the trafficking problem, noting that the "Daily Mail principle does not settle the issue whether, in cases where information has been acquired unlawfully by a newspaper or by a source, government may ever punish not only the unlawful acquisition, but the ensuing publication as well." n129 In this posture, both sides could claim the words of the prior cases; they were not enough alone to decide the matter.

Third, most of the examples in the Daily Mail cases could arguably be distinguished as having also involved content-based discrimination, at least in the sense of limiting their application to defined subject matter. Cox Broadcasting and Florida Star were both limited to disclosure of the identity of rape victims; n130 Daily Mail involved a prohibition on material about a juvenile offender; n131 Landmark was limited to divulging information taken from a state commission to investigate ethics charges against judges; n132 Butterworth involved disclosure of material in grand jury proceedings; n133 and Oklahoma Publishing, involving a judicial gag order and not a statute, was targeted at disclosures involving a juvenile criminal proceeding. n134 Moreover, **[*1130]** in each of these cases, a news organization was the party seeking disclosure, and in some instances, the prohibition explicitly singled out the media as such. n135

Finally, and most importantly, Bartnicki was the first case in the Daily Mail line that seemed to squarely and forcefully pit against one another in a position of virtual equipoise two constitutional rights: freedom of speech, and "the right to be let alone," described by Justice Brandeis as "the most comprehensive of rights and the right most valued by civilized men." n136 While neither the word "privacy" nor the phrase "the right to be let alone" appears in the constitutional text, n137 it is a right treated with persistent reference in the modern opinions of the Supreme Court. n138 The interlocking First Amendment freedoms of speech and association have long been understood as having both positive and negative poles: the freedom to speak incorporates a freedom not to, n139 the freedom to associate encompasses a right of nonassociation, n140 and both speech and association are buttressed by **[*1131]** rights to speak and associate anonymously n141 and in confidence. n142

The "right to be let alone" is not just a right to contemplative silence, it is a right that at times affirmatively encourages expression. Privacy has an empowering quality: it supplies an emancipating permission to speak freely. It is only human nature to speak differently in confidence than one does in public. n143 Whether or not this is an entirely admirable human trait, it is an enduring one. n144 None of us wants to be the object of surveillance or eavesdropping. None of us, from the common citizen to the Commander-in-Chief, wants our private conversations broadcast to the world. n145 Even fear of disclosure after one's own death may temper candor. n146 There is **[*1132]** simply no doubt that adding a prohibition against "downstream disclosure" of illegally intercepted communications contributes significantly to advancing the cause of privacy. To have one's cell-phone conversation intercepted by a geek with a scanner in an unmarked van is one thing; to have the conversation broadcast by Tom Brokaw on the NBC Nightly News or posted on the World Wide Web is quite another. n147 To say the least, the subsequent dissemination compounds the injury. n148 Indeed, it may define its very soul and sinew. n149 And while constitutional law ought not be decided by either opinion poll nor a roll call of the states, the social policy consensus underlying the judgment that it is wrong to traffic in illegally intercepted electronic communications is evidenced by the overwhelming number of states with legislation similar to the federal model. n150

6.Deterrence, Drying the Market, and the Exclusionary Rule Analogy.

- Outside the realm of communication, legislatures routinely make the judgment that it is as important to dry up the market for contraband as it is to attack its initial creation. n151 At times, most notably when approving laws attacking pornography, the Supreme Court has accepted the "dry up the market" rationale even when dealing with speech. In Osborne v. Ohio, n152 the Supreme Court held that the rule of Stanley v. Georgia, n153 protecting "home possession" of obscene material, did apply to possession of child pornography. n154 In Stanley the State of Georgia primarily sought to proscribe **[*1133]** the private possession of obscenity because it was concerned that obscenity would poison the minds of its viewers. Conversely, in regulating possession of child pornography, the government in Osborne was able to rely on more than a mere paternalistic interest in regulating the possessor's mind - it could, rather, defend its law

in the hope "to destroy a market for the exploitative use of children." n155

The question in Bartnicki might thus be answered in purely empirical terms. One might simply seek to determine whether the exclusion of further dissemination is in fact likely to dry up the market and thereby deter illegal interceptions. Posing the question in this way invites a comparison with exclusionary rule jurisprudence, not so much because the two bodies of law bear on one another in a linear way, but rather for what is revealed in contrasting and comparing them.

In Fourth Amendment jurisprudence, the exclusionary rule prevents the introduction of evidence against a defendant in a criminal trial when that evidence is the product of an illegal search or seizure. n156 At the threshold, the analogy to privacy-protective laws such as Title III seems potentially productive, for courts have consistently used Title III to enforce a "fruit of the poisonous tree" norm, even when the intercepted communication is used for what are arguably beneficial and otherwise legal social ends. n157

The "fruit of the poisonous tree" doctrine - that the government may not benefit from evidence obtained illegally, or from evidence developed as a result of the illegal search - traces back to principles first articulated by Justice Oliver Wendell Holmes. n158 Holmes saw the doctrine as integral to **[*1134]** the Fourth Amendment, for without it, the Amendment was reduced "to a form of words." n159

Fundamental to the "fruit of the poisonous tree" concept, of course, is the threshold determination that the predicate conduct - the metaphorical tree - was itself poisonous. n160 But once that is established, should it matter whether the person using the forbidden fruit is also the person who plucked it? The response to this question may be influenced by whether the question is perceived to be empirical or moral. Should the animating principle undergirding the exclusionary rule be understood as a matter of mere deterrence, a question that reduces to practical and empirical judgments, or should it be understood as expressing a moral intuition, a concept of moral taint, a judgment that exploiting prior illegality is itself wrong, a violation of decency and fair play, that ought to be condemned?

On the Fourth Amendment side, the moral argument has not prevailed. The exclusionary rule is instead understood as a prudential limitation aimed at deterrence of misconduct. The rule is not itself of constitutional dimension, n161 the Court has explained, and in recent years the Court has been all but openly hostile to the rule, refusing to extend its reach into new arenas, n162 emphasizing that it applies only in situations in which "its remedial objectives are thought most efficaciously served." n163 The exclusionary rule is **[*1135]** generally seen by the Court as harsh medicine that prevents a tribunal from considering reliable, probative evidence, and often allows those who would otherwise be found guilty to escape the consequences of their ill deeds. n164 The Court has thus applied a fastidious and none-too-generous cost-benefit analysis to the rule, refusing to impose it when its perceived deterrence benefits are outweighed by the substantial social costs the rule imposes. n165 Lastly, for almost as long as it has applied the exclusionary rule and the fruit of the poisonous tree doctrine, the Court has also applied what might be called a "silver platter" doctrine. When an independent agent not connected to the government breaks the law and turns incriminating evidence over to law enforcement officials on a "silver platter," there is no violation.

To the extent that the exclusionary rule is invoked as a linear analogy, it thus cuts against holding the media responsible for dissemination of material illegally obtained by others, especially in light of the principle that the rule does not bar the introduction of evidence handed to the police by someone else who has engaged in private misconduct to obtain it. n166 This principle dates back to Burdeau v. McDowell, n167 a case in which the defendant argued that the government should not be permitted to admit into evidence personal private books and papers purloined and stolen from his private safe, which had been drilled into, and his desk, which had been forcibly entered by breaking its locks, by a third party unconnected to the **[*1136]** government. n168 The Supreme Court refused to suppress the evidence, ruling that

having come into the possession of the government without a violation of petitioner's rights by governmental authority, we see no reason why the fact that individuals, unconnected with the government, may have wrongfully taken them, should prevent them from being held for use in prosecuting an offense where the documents are of an incriminatory character. n169

The Supreme Court has never looked back from Burdeau and it continues to be the law. This silver platter exception is usually explained on the simple rationale that only the government can violate the Fourth Amendment, and that invasions of privacy that would offend the Fourth Amendment if carried on by governmental actors are of no constitutional consequence when an independent actor unrelated to the government engages in the violation. n170

That Burdeau remains good law in the sense that it is still orthodox legal doctrine does not mean, of course, that it remains (or has ever been) good law in the sense that it is intrinsically persuasive. Indeed, Justices Brandeis and Holmes dissented in Burdeau, arguing that whether or not the government itself had violated the Constitution, knowing exploitation by the government of evidence seized through theft was simply not right - it shocked the conscience, violated norms of decency and fair play, and undercut the very rule of law:

Plaintiff's private papers were stolen. The thief, to further his own ends, delivered them to the law officer of the United States. He, knowing them to have been stolen, retains them for use against the plaintiff. Should the court permit him to do so? That the court would restore the papers to plaintiff if they were still in the thief's possession is not questioned. That it has power to control the **[*1137]** disposition of these stolen papers, although they have passed into the possession of the law officer, is also not questioned. But it is said that no provision of the Constitution requires their surrender and that the papers could have been subpoenaed. This may be true. Still I cannot believe that action of a public official is necessarily lawful, because it does not violate constitutional prohibitions and because the same result might have been attained by other and proper means. At the foundation of our civil liberty lies the principle which denies to government officials an exceptional position before the law and which subjects them to the same rules of conduct that are commands to the citizen. And in the development of our liberty insistence upon procedural regularity has been [a] large factor. Respect for law will not be advanced by resort, in its enforcement, to means which shock the common man's sense of decency and fair play. n171

No one has ever persuasively answered Holmes and Brandeis on this point. For the media to invoke by analogy this exception to the exclusionary rule is for the media to act every bit as hypocritically and arrogantly as the government prosecutors who prevailed in Burdeau. It is to say nothing less than that in America, neither the press nor the police have any obligation to play fair.

Even if deterrence and not morality is to serve as the basis for making the judgment as to whether to impose a rule of exclusion for privacy contraband, making the deterrence judgment is nothing approaching an exact science. At the outset, it should be noted that while there is precedent for tying First Amendment inquiries to such empirical judgments, the wisdom of such constitutional tying arrangements is cloudy at best. There are perils to resting constitutional law principles on empirical judgments; social science evidence is often a moving target, an ever rolling and contingent assessment of new surveys and studies or new interpretations of old surveys and studies. The stability of constitutional law is threatened if doctrines must be adjusted each time the results change. The role of empirical evidence in constitutional law is thus itself a highly problematic matter; perhaps the most that can be said is that the quantum and quality of empirical evidence required persuasively to support or overcome a proffered right will vary with other circumstances of the case, including such factors as the novelty or inherent logical sense of the argument. n172

From the self-interested perspective of the media, moreover, linking constitutional doctrine to social science data also poses the tactical risk that the data will prove unfavorable, if it proves much at all. In Branzburg v. Hayes, n173 for example, the Court appeared to reject the notion of a First **[*1138]** Amendment-based "reporter's privilege," which would shield reporters from providing testimony in criminal trials that would reveal their confidential sources. n174

One of the principal rationales relied upon by Chief Justice Burger in his opinion for the Court was his skepticism that such a reporter's privilege was necessary to ensure effective newsgathering. Journalists argued that without being able to extend to reluctant sources promises of confidentiality that legal tribunals would be required to respect, sources would dry up, whistleblowers would not whet their whistles, and newsgathering would be crippled. The Supreme Court did not buy the empirical argument, and seemed to reject the privilege, though lower courts would not interpret the decision quite so cleanly. n175

So too, in Red Lion Broadcasting Co. v. FCC, n176 broadcasters resisted the imposition of the "fairness doctrine" (requiring that both side of controversial issues be presented) upon them on the theory that it would act perversely, actually discouraging broadcasters from presenting controversial material. Again the Supreme Court did not buy the argument, though it left the door open for reconsideration of the question if upon further review the empirical case for such a backlash effect could be made. n177 Similarly, the defamation standard emanating from New York Times Co. v. Sullivan n178 is based in part on an empirical judgment that without the provision of a fault standard for libel set higher than ordinary negligence, journalists would engage in self-censorship when reporting about public officials and public figures on matters of public concern, to avoid the possibility of judges and juries finding them liable for negligence as they examine their actions after **[*1139]** the fact. n179 Yet if the Supreme Court ever required genuine hard evidence that the "chilling effect" of the negligence standard repudiated in New York Times actually exists, the media might well be fearful that the evidence could not be garnered. n180 The point here is not that the New York Times rule is indefensible - it is better described as indispensable n181 - but rather that its defense is more comfortably made by arguing principle than sociology. n182

In the specific context of trafficking in privacy contraband, the media can certainly attempt to gain some argumentative purchase from the fact that there is no body of data demonstrating that the opportunity to sell or donate stolen communications encourages a "market for surreptitious and illegal electronic surveillance. As a matter of common sense, it seems highly unlikely such data could ever be produced; there is a lot of surveillance going on, with all those millions and millions of scanners out there, and only a trickle of it ends up as broadcast news. n183 On a nonquantitative level, however, there is something to the "drying up" argument, something tied to the creeping tabloidization of modern American mass culture.

Those who intercept cell phone communications for passing sport are perhaps not the private-space invaders about whom we should be most concerned. **[*1140]** Rather, the real worry lies with those who have some axe to grind and actually target identified victims for electronic stalking. These eavesdroppers are the ones most likely to have some motivation to use and abuse that which they intercept, including the motivation to drop the material on the doorstep of media outlets. As to this smaller group of invidious interceptors, the presence of a liability-free media ready to publicize the intercepted material in the happy comfort of legal immunity may well create an incentive for invasion, and penalizing disclosure may well, as to this smaller group, work effectively to dry up, if not entirely dry out, that high-visibility submarket.

Unfortunately, Justice Stevens's majority opinion in Bartnicki barely scratched the surface of these problems. The Court seemed to have a fundamental difficulty with the drying up argument, because it punished the "innocent" receiver and disseminator of the unlawful interception rather than the true culprit in the escapade, the actual wrongdoing interceptor. This ran afoul of what the Court appeared to regard a baseline norm: that as law exists to deter transgression, it should punish actual transgressors. n184 If the sanctions that presently attach to a violation of laws prohibiting electronic interceptions are not up to the trick, the Court suggested, "perhaps those sanctions should be made more severe." n185 To go so far as to punish the speech of the law-abiding to deter the iniquitous conduct of law breakers, the Court insisted, would be "quite remarkable." n186 With rapid strokes, the Court dismissed the analogy to child pornography with the epithet that child pornography was, after all, low-value speech "considered of minimal value." n187 And as for other cases in which the criminal law punishes those who receive stolen goods so as to dry up the market for trafficking in such goods, the Court summarily declared that because those examples did not involve speech, they were simply irrelevant to First Amendment analysis. n188

Thus the Court reasoned that the drying up rationale would be defensible only if one could make a case that for some reason it is especially difficult to find and punish interceptors, or make a case that interceptors do their intercepting largely to obtain the benefits of revelation to third parties, so that a prohibition on disclosures would have a corresponding benefit in deterring interception. But the Court found no evidence Congress viewed the prohibition against disclosures as a response to the difficulty of identifying persons making improper use of scanners and other surveillance devices, and concluded there was "no empirical evidence to support the assumption **[*1141]** that the prohibition against disclosures reduces the number of illegal interceptions." n189

7.The Newsworthiness Trump Card - Comparing the Plurality, Concurrence, and Dissent.

- Although Justice Stevens's opinion was utterly uncharitable toward the "drying up" argument, it was less parsimonious in its acceptance of what might be called the "compounding" argument - the notion that the widespread dissemination of intercepted material substantially compounds the injury to privacy. In its general introductory remarks, the Court acknowledged that the case presented "a conflict between interests of the highest order - on the one hand, the interest in the full and free dissemination of information concerning public issues, and, on the other hand, the interest in individual privacy and, more specifically, in fostering private speech." n190 When the Court turned to a more detailed analysis of the "compounding" argument, it acknowledged that the government had at least an "important" interest in acting to preserve the privacy of communication. n191

Despite these acknowledgments, there was nothing in the Court's treatment of the privacy interests at stake in Bartnicki that one could properly call resonate. The nods to privacy seemed perfunctory and obligatory, if not downright miserly, and they were rather easily trumped. In a cursory analysis, the Court reasoned that the privacy interests at stake were outweighed by the First Amendment interest in permitting the dissemination of newsworthy information, and that the intercepted statements pilfered from the private conversation between Bartnicki and Kane were newsworthy because they would have been so classified had they been made in an open public arena. n192 This was a disappointing analysis, at once mechanical and superficial. When one contrasts it to the analysis made by five other Justices in the case (Justices Breyer and O'Connor in concurrence, and the Chief Justice and Justices Scalia and Thomas in dissent), one may venture more: Justice Stevens's analysis on this point is not truly the holding of the **[*1142]** Court.

The concurring opinion of Justices Breyer and O'Connor was far more constrained than the opinion of the Court in substance, in tone, and in the signals it might fairly be read to have been making for future cases. n193 The holding, Justice Breyer insisted, was limited to the "special circumstances" the case presented, in which "the radio broadcasters acted lawfully (up to the time of final public disclosure)" n194 and the information broadcasted "involved a matter of unusual public concern, namely a threat of potential physical harm to others." n195 Note the emphasis added in the just-quoted caveat, in which Justice Breyer spoke of the case as involving a matter of "unusual" public concern, and then identified what was so unusual about it - a threat of potential physical harm to others.

As Justice Breyer saw the matter, the case posed a true constitutional conflict, involving competing constitutional values - indeed, competing First Amendment values, the right of the media to publish information on the one hand, and the "right to be let alone," which in turn serves the First Amendment interest in fostering private speech. n196 The strict scrutiny standard was out of place in such situations, Justice Breyer reasoned. Rather, with interests of constitutional dimension on both sides of the equation, a balancing methodology that gave meaningful weight to both of those dimensions was called for. Using a First Amendment cost-benefit analysis, Justice Breyer stated that he

would ask whether the statutes strike a reasonable balance between their speech-restricting and speech-enhancing consequences. Or do they instead impose restrictions on speech that are disproportionate when measured against their corresponding privacy and speech-related benefits, taking into account the kind, the importance, and the extent of these benefits, as well as the need for the restrictions in order to secure those benefits? n197

The statutory restrictions, Justice Breyer argued, are designed to assure us a measure of privacy that "helps to overcome our natural reluctance to discuss private matters when we fear that our private conversations may become public." n198 In this sense, the statutory restrictions actually serve to "encourage conversations that otherwise might not take place." n199 As Justice Breyer appeared to see the matter, the restrictions the statutes place on speech were at once deliberate and necessary, operating not merely as a **[*1143]** means but as an end. n200 For "media dissemination of an intimate conversation to an entire community will often cause the speakers serious harm over and above the harm caused by an initial disclosure to the person who intercepted the phone call." n201

The intramural interceptor may be doing little more than imbibing in the passing thrill of eavesdropping, an electronic "listening Tom" getting cheap thrills from fragments of randomly captured conversation. The interceptor who passes information on to the mass media, however, is playing varsity ball. Whether or not many intercepted phone calls ever get disclosed in the major channels of mass media, the possibility alone is chilling. As Justice Breyer observed, the "threat of ... widespread dissemination can create a far more powerful disincentive to speak." n202

Whereas the opinion for the Court by Justice Stevens emphasized the Daily Mail line of cases and the presumptive unconstitutionality of laws that burden trafficking in truthful information, Justice Breyer's opinion adopted exactly the opposite baseline. Laws protecting private electronic conversations, like "laws that would award damages caused through publication of information obtained by theft from a private bedroom," must as "a general matter" be tolerated by the First Amendment, he argued, because of the importance of privacy, including its role in fostering private speech. n203 In Justice Breyer's view, the question was merely one of balance and tailoring; the Constitution does not broadly forbid legislation against trafficking in privacy contraband, it merely "demands legislative efforts to tailor the laws in order reasonably to reconcile media freedom with personal, speech-related privacy." n204

And therein was the crux of the concurring views of Justices Breyer and O'Connor. Their quarrel was not with the general principle of banning the disclosure of illegally intercepted communication, but with the specific balance struck by the statutes being reviewed, as applied to the specific factual circumstances in Bartnicki, circumstances the two concurring Justices viewed through a prism of factual assumptions that cast them in their most sinister possible light. The statutes, as applied, failed to "reasonably reconcile" the competing interests, interfering "disproportionately" with "media freedom." n205

The broadcasters, Justice Breyer noted, did not "encourage[]" or "participate[] **[*1144]** directly or indirectly in the interception." n206 "No one claims that they ordered, counseled, encouraged, or otherwise aided or abetted the interception, the later delivery of the tape by the interceptor to an intermediary, or the tape's still later delivery by the intermediary to the media." n207 This observation suggested that in Justice Breyer's view, any such involvement by the media would have disqualified it from the protection the Court granted in Bartnicki, and rendered the media answerable under the statutes.

In a particularly intriguing discussion, Justice Breyer also emphasized that the laws at issue did "not forbid the receipt of the tape itself." n208 Justice Breyer seemed to be signaling that if the law made it illegal to receive the actual tape recording, to obtain it (at least with knowledge that it contained illegally purloined conversations) would itself be unlawful conduct. In such a case, Justice Breyer appeared to be arguing, the media could no longer claim the safety-base of having acquired the information "lawfully," and would now be outside the ambit of the Bartnicki protection. n209 If this is what Justice Breyer in fact meant, he had identified a sizable constitutional loophole, and all but invited legislatures to amend their statutes and drive through.

Justices Breyer and O'Connor seemed offended by the conversation between Gloria Bartnicki and Anthony Kane, treating it not as angry "union-talk" but as actual authentic discussion of the need to engage in violence against persons and property. Had Bartnicki and Kane been merely expressing their anger at the school board for its negotiating positions, Justices Breyer and O'Connor might not have gone along with Justices Stevens, Ginsburg and Kennedy, and instead defected to the camp of the Chief Justice, and Justices Thomas and Scalia. It was The Sopranos talk of blowing

off porches and "doing some work on some of these guys" (or "dese guys") that appeared to overwhelm Justices Breyer and O'Connor, leading them to the view that "the speakers had little or no legitimate interest in maintaining the privacy of the particular conversation." n210 Noting that in other contexts in which the law normally respects the confidentiality of private conversations, exemptions exist permitting or even requiring disclosure in the interest of public safety, Justices Breyer and O'Connor found that the threat of violence, even if it had grown somewhat stale with time, trumped the privacy interests of the parties to the conversation. n211

[*1145] Justices Breyer and O'Connor also emphasized that Bartnicki, the union's chief negotiator, and Kane, the local union's president, were "limited public figures," in the parlance of defamation law, having "voluntarily engaged in a public controversy ... thereby subjecting themselves to ... greater public scrutiny" and diminished expectations of privacy. n212 The problem with relying on the "limited public figure" status of Bartnicki and Kane to justify the privacy invasion, however, was one of scope. Undoubtedly it is true that Bartnicki and Kane opened themselves up to greater public scrutiny for their statements in public arenas regarding the union dispute. That is certainly part of the American bargain. But it is not at all clear that having one's conversations surreptitiously intercepted and broadcast to the world is part of that bargain, even when the conversations are germane to the public issues and public controversies that form the predicate of the plaintiffs' public figure status. Judges and their law clerks are public officials, and what they say in conversations about pending cases are clearly statements on "issues of public concern," but it is a high stretch to imagine that illegal tape recordings of private exchanges between judges and clerks in which they think no one is listening carry the same diminished expectation of privacy as conversations made in more public arenas. Putting the matter more generally, all of us talk all of the time on "issues of public concern" in private conversations, where we may dare to be vulgar, profane, irreverent, politically incorrect, off-the-wall, angry, comedic - whatever - thinking we are outside of public scrutiny and off the public record and able to let our hair and defenses and masks down and let it all hang out. What we say in these moments may not even be our true feelings; they may just be our raw feelings, or perhaps not our feelings at all, just things said to be funny or outrageous, to posture, to impress, or to just push our listener's buttons.

There was, in short, a lameness to the assertion by Justice Stevens that anytime an otherwise private conversation implicates matters of public concern, freedom of speech must trump the right to privacy. n213 And while Justice **[*1146]** Breyer's opinion trimmed Stevens's point, even his concurring opinion may not have trimmed it enough. Justice Breyer was careful to admonish, however, that his judgment that the public figures Bartnicki and Kane had forfeited their privacy rights in their particular conversation was "not to say that the Constitution requires anyone, including public figures, to give up entirely the right to private communication, i.e., communication free from telephone taps or interceptions." n214 In an extremely significant passage, in fact, Justice Breyer's opinion seemed to signal that he agreed with decisions (rare as they are) in which courts have held that sensationalized accounts of the "truly private" aspects of even a celebrity's life - such as his or her sexual relations - ought not qualify as speech "on matters of public concern" for First Amendment purposes. n215

In what was patently a well-calculated exercise in spin (or damage) control, Justice Breyer thus characterized the Court's opinion, which he described as finding that a limited constitutional privilege to publish unlawfully intercepted conversations "of the kind here at issue," did not create an omnibus ""public interest' exception that swallows up the statutes' privacy-protecting general rule." n216 Instead, as Justices Breyer and O'Connor conceptualized the Court's holding, the Court had merely acknowledged a narrow realm of First Amendment shelter "for publication of intercepted information of a special kind." n217 In Justice Breyer's view of the case, the outcome in Bartnicki did not present the rule but the exception, a situation in which the "speakers' legitimate privacy expectations are unusually low, and the public interest in defeating those expectations is unusually high." n218

Elaborating on the loophole his opinion had previously suggested, n219 Justice Breyer ended by emphasizing his view that "the Constitution permits legislatures to respond flexibly to the challenges future technology may pose to the individual's interest in basic personal privacy." n220 The inexorable advance of technology raises the possibility of "clandestine and pervasive invasions of privacy" more onerous than we may at present even **[*1147]** be able to imagine. n221

Most of us today are relatively free and easy with our cellular phone conversations, chatting away foolishly, insouciantly oblivious to all those prurient eavesdroppers who with their modified Radio Shack scanners are listening to all we say. At one point in Justice Breyer's opinion, he almost seemed to opine that cell phone talkers this negligent get what they deserve. n222 But what will happen when privacy-defending technologies, such as encryption devices, come into the market with more widespread adoption, so that the privacy invaders must escalate their espionage to new levels of aggressiveness in order to invade privacy rights that the electronic conversants have now gone to much greater energy and expense to secure? Justice Breyer left open the distinct possibility that legislatures could respond to these privacy techno-wars with measures designed to protect privacy that might include limits on disclosure, and that in such circumstances the appropriate First Amendment balance might well be different. n223

Three Justices - Chief Justice Rehnquist, and Justices Scalia and Thomas - saw no need to wait. Chief Justice Rehnquist's dissent took up many of the same themes as Justice Breyer's concurrence, but drove them each one step closer to home. "Technology now permits millions of important and confidential conversations to occur through a vast system of electronic networks," the Chief Justice observed. n224 "These advances, however, raise significant privacy concerns," he continued. n225 "We are placed in the uncomfortable position of not knowing who might have access to our personal and business e-mails, our medical and financial records, or our cordless and cellular telephone conversations." n226 The laws at issue, he argued, were content neutral; they sought to restrict only the disclosure of information that was illegally obtained in the first instance, they placed no restrictions on republication of material already in the public domain, they did not single out the media for especially disfavored treatment, they utilized a scienter **[*1148]** requirement to avoid being sprung to trap the unwary, and they promoted both the privacy interests and the free speech interests of those using devices such as cellular telephones. n227

The cases in the Daily Mail line, the Chief Justice argued, all defined their coverage by content or subject matter instead of by source, and were by those elements alone distinguishable. n228 More importantly, however, the Chief Justice disagreed with the majority's conclusion that Daily Mail line of cases applied to all receipt of "truthful" information. In each of those cases, he pointed out, the media had obtained the information from the government itself. n229 In each case, the material was either a matter of public record, a status that would appear to indicate that the government has reached the conclusion that the public interest is served by public access to it, or the information was obtained by the media through a "leak," either intentional or inadvertent, by a government employee or agent. The government could thus seek to vindicate its interests by working harder to ensure its own security, or by punishing its own agents or employees. n230 Moreover, in each case, the information "was already publicly available, [so that] punishing further dissemination would not have advanced the purported government interests of confidentiality." n231 The statutes, the Chief Justice noted, prohibit "disclosure," and one cannot disclose that which is already public. n232

Most important, to the extent that the laws in prior cases were seen as violating the First Amendment because they threatened the media with "timidity and self-censorship," the Chief Justice argued, here the tables were turned, for here the statutes actually acted to alleviate the "timidity and self-censorship" that might plague private conversations, by subjecting them to the big chill of illegal interception and public disclosure. n233

One of the infirmities the Court had found with the statute in Florida Star was its lack of any intent requirement. n234 Antitrafficking statutes, however, do impose various forms of scienter, generally addressing only those who knowingly disclose an illegally intercepted conversation. n235

The Chief Justice found it incredible that the Court would place weight **[*1149]** upon the fact that the receipt of an illegally intercepted communication is not itself a criminal act. For the fact that receipt of stolen material is not technically criminal does not necessarily mean that the knowing receipt and additional disclosure of such information is appropriately labeled "law-abiding." n236 For after all, the Chief Justice reasoned, "transmission of the intercepted communication from the eavesdropper to the third party is itself illegal," and thus when "the third party [later] knowingly discloses that communication," it is a fair characterization to say that yet "another illegal act has been committed." n237 This situation, the Chief Justice argued, is distinguishable from cases in which a journalist lawfully obtains "information through consensual interviews or public documents." n238

Unlike the majority, the dissenters found the "dry up the market" theory "neither novel nor implausible," but rather "a time-tested" concept that undergirds many venerable laws, including the ancient "prohibition of the knowing possession of stolen goods." n239 While the transference of the content of intercepted information may not be exactly analogous to the transfer of stolen physical property, it has many of the same attributes, and without limitations on downstream transfer and disclosure invidious interceptors may accomplish their ultimate goal through the simple expedient of "laundering the interception through a third party." n240 To the victim of the privacy invasion, there is little solace in the smug defense that one's private conversations were first laundered through another before being broadcast to the world. The Chief Justice also pointed out that laws promoting privacy in cell phone conversations protect privacy on an entirely different scale than the laws at issue in cases such as Daily Mail, for those cases involved laws that "served only to protect the identities and actions of a select group of individuals," whereas electronic privacy "laws protect millions of people who communicate electronically on a daily basis." n241

F. The Bottom Line: Reading Bartnicki as a Backhanded Victory for Privacy

When one processes the ambiguous points of Justice Stevens's opinion, the trimming observations of Justices Breyer and O'Connor, and the views of the dissenters to the extent that they support the "Court" lead by Breyer and O'Connor, Bartnicki no longer seems like a defeat for privacy **[*1150]** protection, but an opinion more in the nature of a backhanded victory. The decision does not shut the door on the prohibition of privacy contraband - at the very least it keeps the constitutional status of privacy contraband largely in play.

If we are to take privacy seriously, this continued play is a good thing. From the broadest perspective, Bartnicki accepted the premise that the conflict posed between speech and privacy is a conflict between two rights of constitutional stature. By this important measure, all nine Justices in Bartnicki were in agreement. It was by no means clear that consensus on this broad philosophical point would emerge. It has been forcefully argued that treating the balance between privacy and speech interests as a conflict between two constitutional rights is misleading and wrong, because the Constitution only prohibits restrictions on speech or invasions of privacy by the government, and is silent about similar restrictions when they come from private actors. n242 Moreover, the fact that private actors may engage in expressive activity that offends constitutional values such as equality or tolerance has not been traditionally understood as a sufficient basis for abridging speech. We permit private speakers to engage in speech that is racist or religiously intolerant, even though racial equality and religious tolerance are, in a general sense, treasured "values" in our constitutional system. n243

The Court in Bartnicki clearly saw the case before it, however, as different from the hate-speech example. A restriction on hate speech prevents a private speaker from speaking his or her mind in a public arena because the government disagrees with the speaker's message. Upholding a restriction on privacy contraband, however, merely permits the government to come to the aid of a speaker who has not expressed himself or herself in a public arena and who does not wish to have his views involuntarily exposed from having those views forcibly stolen and disseminated. The "newsworthiness" principle emerged as the key doctrinal mediator in this conflict, and on this point the pivotal opinion of Justices Breyer and O'Connor is particularly important. (The "newsworthiness" defense as used here does not refer to the sweeping version of the defense in Justice Stevens's opinion, but the far narrower rendition employed in the opinions of Justice Breyer and Chief Justice Rehnquist.) A tally of the concurring opinion and the dissent generates a total of five Justices who endorse the principal ingredients of the "publication of private facts" tort, with its "newsworthiness" defense built in, as it exists at common law. n244 For those Justices, there is nothing at all constitutionally offensive about empowering judges **[*1151]** and juries to make the judgment that a particular fact revealed by the media is not newsworthy. n245

There is some measure of irony here. A privacy contraband triggered only by the source of information is genuinely content neutral, and thus most strongly deserving of the benefits of some lower level of constitutional scrutiny, such as intermediate review. n246 Privacy laws that narrow their reach to prohibit trafficking only in material that is not "newsworthy," however, are by definition content based. n247 On a surface level, it might be thought that laws that deal only with how the material was gathered would seem to be less offensive to the First Amendment because they are

content-neutral. But the matter is not so clean. The use of content in privacy-protection laws often operates to narrow very significantly the reach of the law, and so to that extent the content-based coverage limitation actually reduces (at least by a purely quantitative measure) the impact on free expression. n248 There may be other risks incident to this use of content to define the scope of the law that nevertheless justify closer judicial scrutiny of such content-based limitations, but it is important to see that the use of content as a cabining device is not entirely without its constitutional benefits. Moreover, the invocation of content in such privacy laws does not carry a particularly invidious tint. To the contrary, content is usually used in such laws to attempt to encapsulate the legislature's judgment as to the types of information that are sufficiently "private" to merit the law's protection in the first place. A legislative prohibition on unauthorized trafficking in an patient's medical records, a student's academic records, or photographic or sound images capturing a person engaged in sexually intimate or familial activity, all add an element of "content" definition to a privacy law. But to the extent that the use of content in such laws confines their coverage to the vindication of the privacy objectives at which the laws are aimed, the use of **[*1152]** content arguably enhances First Amendment values more than it detracts from them, by employing greater precision in regulation.

Still, it is worth observing that the kind of "newsworthiness" judgment the common law has traditionally required in the context of the "private facts" tort, and that the five concurring and dissenting Justices in Bartnicki would seem to have superimposed upon laws such as Title III, actually works to turn otherwise content-neutral laws into content-based ones. In this observation, there is a clue to how the principles in Bartnicki might apply in other information-contraband situations, such as intellectual property law. For it quite emphatically does not appear that Justices Breyer and O'Connor, or any of the dissenting Justices, envisioned that their version of "newsworthiness," when added to the assessment, would simultaneously elevate the level of judicial scrutiny. Indeed, the opinions of the five concurring and dissenting Justices would collapse on themselves if this were what they meant, for the very device used to strike the "reasonable" balance between privacy and speech those Justices would employ - the newsworthiness defense - would simultaneously tilt the balance entirely in favor of speech, by treating the now-revised law as content based, thereby upping the ante of judicial review to strict scrutiny.

Rather, the newsworthiness defense as contemplated by the five concurring and dissenting Justices must be understood as itself striking the appropriate constitutional balance, as the load-bearing doctrinal substitute for strict scrutiny. This understanding of the concurring and dissenting opinions in Bartnicki is not only internally coherent, it is externally harmonious with comparable devices used in other areas of First Amendment law. Much like the "fair use" defense in copyright, or the "newsworthiness" defense in common-law appropriation cases, or the "public controversy" doctrine in defamation law, the newsworthiness defense contemplated in Bartnicki invokes a content-sensitive test to separate that which deserves protection from that which does not.

There is a great deal of emphasis in modern defamation law on "voluntary" entry into a public controversy as an important factor (indeed, often a controlling factor) in saddling a plaintiff with the status of "limited purpose public figure." There may, however, occasionally be "involuntary" public figures, as when a criminal engages in illicit actions and seeks all the while to avoid public scrutiny, but is ultimately exposed. The criminal did in such cases "volunteer" for the activity that became a public controversy when it was revealed, and there are not many equities on the criminal's side when media attention is focused on those activities. If one really believes that Bartnicki and Kane were like criminals plotting violent conspiracies to blow up porches and bust up people, then the "involuntary public figure" label might apply. This seems to have been what Justices Breyer and O'Connor believed. If, on the other hand, one is more inclined to think that Bartnicki and Kane were simply letting their anger, frustration, and perhaps their fantasies flow uninhibited, thinking they were venting, one compatriot **[*1153]** to another, in the security of a private conversation, it becomes very difficult to make a convincing case that Bartnicki and Kane had in this conversation entered the arena of public controversy. If that is the law, then public figures - even limited purpose public figures - are reduced to zero legitimate expectation of privacy in even their private conversations, if those private conversations are generally on the subject matter of a larger public controversy in which they are participants. This ought not be the law, and one hopes Bartnicki has not made it so. Limited purpose public figures may volunteer for increased public scrutiny, but they have not volunteered for total surrender of their human dignity. It is hard enough to convince good people to enter the arenas

of public life, accepting the "bargain" of diminished privacy in exchange for enhanced influence. This makes the contract unconscionable. n249 As the Chief Justice noted in dissent, "Bartnicki and Kane had no intention of contributing to a public "debate' at all." n250

To the extent that five Justices in Bartnicki might be understood as inviting the importation into First Amendment jurisprudence of the "newsworthiness" analysis as it has developed so far in common-law cases (where courts normally treat the defense as an amalgam of constitutional and common-law principles), it will become important to ask whether such familiar tort principles as risk-assessment and risk-spreading will also become part of the mix. In First Amendment parlance, this in turn invokes the "media-nonmedia" distinction.

In a relatively casual announcement, the Court stated that it treated Yocum, the individual defendant, and the various media defendants as equivalent for its analysis of the case, refusing to draw any distinction between them. n251 The Court thus conjured, but did not seriously address, a long-standing debate over whether the First Amendment contains any special protections for the institutional press. The problem of whether any special First Amendment privileges should protect the media as institutions is central to the "reporter's privilege" cases, in which journalists seek a special testimonial exemption from revealing confidential sources or other material obtained during newsgathering. n252 It is also important in the context of "access" cases, in which the press seeks special rights of access to public institutions (such as prisons) or locations such as military operations (such as access to the battlefield) beyond that granted to the general public. n253 Figuring **[*1154]** out what posture to take in these debates can be a tricky dilemma for media organizations and journalists, as a matter both of principle and long-term litigation strategy. Generally First Amendment advocates believe in a seamless First Amendment, one that does not look kindly upon distinctions among speakers or different media. n254 At the same time, without some concept of a two-tiered First Amendment that creates some unique protections for the institutional press over and above those enjoyed by the general public, it is difficult to build a coherent case for the "reporter's privilege" or special claims of media access. n255

The Bartnicki case exposes the counter-pressures in this debate. One of the arguments against a two-tiered First Amendment is that recognition of special First Amendment for the institutional media might imply a corresponding legitimacy to the recognition of corresponding responsibilities. These responsibilities might be understood as hortatory, the civic lectures of civic journalism, or they might be understood as legally enforceable incidents of a privileged position, the responsibilities of public trustees. Among the distinctions that might be drawn on the negative side of the ledger is that the media have a capacity to inflict damage far more vast than anything a private individual might normally cause, an exponentially greater capacity, for example, to invade privacy, and to compound the humiliation and anguish caused by such invasions. This might be invoked to justify greater exposure to tort liability. Given that invasion of privacy is, in one respect, part of the "business" of the media, in both an economic and professional sense, in that the media exist (by their own proclamation) in part to bring into the public light those newsworthy aspects of private life that deserve the attention and critique of the larger community, one might plausibly treat as a "cost of doing business" the payment of money damages to individuals who have their privacy interests damaged when the calculations go awry. By analogy to products liability theory, the media might be **[*1155]** seen as the better entities for calculating and spreading the social costs incurred by privacy invasions, so that when the occasional wrongful invasion causes injury, just as the occasional defective product causes injury, liability rules are set so as to make the media the presumptive insurers.

When one starts thinking creatively about these analogies, the chess game deepens. For in the context of products liability, there is a longstanding subdebate over how to handle the unavoidably dangerous product. n256 Certain products carry with them an inherent risk that cannot be eliminated by any known technology or design. Sometimes it is possible to draw the conclusion that the social utility of the product cannot justify the risks imposed, in which case the law may choose something close to absolute liability on the product's manufacturers, or permit the manufacturer to shift that liability through warnings that place an assumption of risk on the consumer. The debate over the proper standard in such cases is usually fought on somewhat different ground when the social utility of the product dramatically outweighs the projected accident costs, as when the product is a drug or medicinal device that is highly efficacious but that produces some small risk of side effect for some consumers that cannot be eliminated. n257

If the media are engaged in the "product" of news and if the process of gathering that news is in part a process undertaken for the greater good of the democracy, the question of how to assign "accident costs" for the invasions of privacy that in hindsight appear to have been unwarranted and gratuitous could be reduced to the same kind of calculations used in the product cases. The news is not just any product, the argument might be, but a highly important one, the equivalent of blood or life-saving drugs, in which there is a constant need but also a constant risk of unfortunate side effect. n258 Consumers, however, do not "choose" this product in quite the same way they choose a blood transfusion or medicine. The community, however, might be understood as making a group choice, a social compact, in which we collectively agree that in return for the collective benefit of newsgathering, we all collectively assume the risk that we might one day find ourselves the victims of gratuitous privacy-invading newsgathering. n259

Continuing to bat this ball back and forth over the net, however, we might still want to ask whether the appropriate social response is a rule of **[*1156]** no liability, in which the media are entirely exempt from accountability for the privacy invasions they should not have made, or whether the insights of tort law outside the realm of speech provide still other useful clues as to lines that might be sensibly drawn. In the case of the unavoidably dangerous product, there is by hypothesis a scientific barrier in play - no test exists for determining whether the product is "tainted" or whether a specific consumer will suffer a certain side effect. n260 Invasions of privacy, however, do not fit easily into this physical-world paradigm, for we are not talking about physical injuries but psychological and social injuries, in which the very notion of a product that is "defective" seems somewhat a play on words. We cannot define "defect" here using the tools of chemistry or engineering. Rather, as previously discussed in connection with the common-law view of the "publication of private facts tort," defining what is "private" or "public" is a matter of social convention, and so is defining what is "newsworthy." n261

II. Other Forms of Information Contraband

Space and prudence caution against attempting to thoroughly analyze here all other forms of information contraband that might suggest themselves, but it is helpful to at least briefly take note of the tensions that exist in dealing with information contraband in other contexts, both for what those tensions reveal about Bartnicki, and for what Bartnicki reveals about them.

A. Intellectual Property Contraband

Intellectual property laws create forms of "information contraband" as a matter of routine, often assigning to owners of intellectual property powerful rights to exclude others from unauthorized trafficking in it. Moreover all intellectual property protection is necessarily content based. Protection of intellectual property without reference to content would be incoherent. Because intellectual property laws, virtually by definition, create limits on trafficking in truthful information, and because they also, virtually by definition, are content based, a simplistic understanding of First Amendment doctrine might lead one to the errant conclusion that the Daily Mail principle, n262 and the "strict scrutiny" test classically invoked to strike down content-based **[*1157]** restrictions on speech, n263 would conspire to render such laws constitutionally suspect. At the very least, one might expect that legislatures and courts, in creating and defining intellectual property rules, would be walking on constitutional eggshells.

Yet in the myriad intellectual property cases it has decided, never once has the United States Supreme Court announced it would subject any provision of federal intellectual property law to the First Amendment's strict scrutiny test. Nor has the Supreme Court subjected state intellectual property laws to strict scrutiny. This striking fact tells us something valuable about how Bartnicki fits into the broader expanse of First Amendment law.

It would be both impertinent and impractical to superimpose an omnibus "strict scrutiny" standard on the complex statutory schemes characteristic of intellectual property law. A casual browse through modern copyright law, for example, reveals how constantly and inevitably copyright law is crafted with reference to content, with special variations and caveats applicable to all sorts of expression, including literary works, architectural works, pictorial, graphic and sculptural works, factual compilations, musical works, dramatic works, pantomimes and choreographic

works, motion pictures and audiovisual works, sound recordings, derivative works, and countless other categories and subcategories, each reflecting the considered view of Congress (and the interpretative gloss of the courts) on the appropriate balance of societal interests posed by each form and subject of expression. n264 The Supreme Court has never held, or even intimated, that Congress is subject to the searching superintendence of strict judicial scrutiny for every difficult policy choice it makes in defining the laws of patents, trademarks, or copyright. To the contrary, all of our intellectual property jurisprudence suggests that the accommodation between freedom of expression and protection of intellectual property is effectuated in gross, through the large structural elements of intellectual property that serve the function of mediating between ownership in expression and free trade in expression.

While many aspects of intellectual property law reflect this accommodation, it is most famously captured in copyright jurisprudence in two concepts, the "idea-expression" dichotomy and the "fair use" doctrine. n265 Tellingly, these fundamental principles of copyright, fair use and the idea-expression dichotomy, are heavily laden with content-based distinctions. Yet it has never been understood that the "strict scrutiny" test is superimposed on top of those doctrines. Instead, Congress and the courts have engaged **[*1158]** in exactly the opposite assumption, that doctrines such as fair use and the idea-expression dichotomy are the accommodation copyright law makes to free expression. n266

In this regard it is worth comparing copyright law to defamation law. Unlike copyright law, which has largely developed in its own universe without any overt importation of First Amendment jurisprudence, modern defamation law has been heavily constitutionalized, with many common-law defamation doctrines now modified to reflect a greater accommodation of free speech values. n267 There are, however, some useful parallels. The "fact-opinion" dichotomy in defamation law, which immunizes a defendant from liability for statements that are not factual (such as opinions, characterizations, or rhetorical hyperbole), serves much the same "engineering function" as the fair use doctrine serves in copyright law. The law of defamation vindicates an individual's interest in reputation by providing limited protection against false statements of fact, but the law does not protect reputation to the extent of immunizing the individual from nonfactual comment, critique, and criticism. In parallel, the law of copyright protects an author's intellectual property from unauthorized exploitation, but does not protect that property from copying incident to comment, critique, and criticism. While the First Amendment does require that state defamation law be limited **[*1159]** to false assertions of "fact," n268 American courts have never held that the actual doctrinal content of the "fact-opinion" distinction as it exists in defamation law is subject to the overriding "macro-doctrine" of First Amendment "strict scrutiny." Indeed, any such attempt would result in utter doctrinal chaos. Thus, it has always been understood that the substance of the "fact-opinion" doctrine itself supplies the First Amendment standard. From a First Amendment perspective, the Supreme Court requires that states impose defamation liability only for false statements of fact; beyond that minimum, states are left to themselves to craft the precise contours of the "opinion" defense. n269 The methodology of "strict scrutiny" (or even "intermediate scrutiny," for that matter) is simply irrelevant. A similar mechanism operates in copyright law. While the Supreme Court has stated that the idea-expression dichotomy and the fair use doctrine eliminate any tension between copyright law and the First Amendment, the Supreme Court and the uniform jurisprudence of lower courts have never treated the First Amendment as an independent font of detailed copyright doctrine (or even intimated such a principle), but instead has assumed that sufficient protection for freedom of speech inures in the structure of copyright law itself.

Defamation law, it is also worth noting, has an "antitrafficking" doctrine of sorts. It is a basic axiom of libel law that a publisher is not absolved of liability for libel merely because the libelous statement is attributed to a source. Rather, the long-standing principle of defamation law is that the repeater of the libel "adopts it as his own," on the logic that "talebearers are as bad as talemakers." n270 The repeater is responsible for the defamation even though it may be attributed to a source. n271 Thus, just attributing otherwise false and libelous statements to another does not render those statements "substantially true," or immune from liability. This principle applies to libels published by the press just as it does to back-fence **[*1160]** slander. n272 On one level, this is an imposition of liability for trafficking in the "truth," the "truth" being the literal fact that the source in fact said what the publisher says the source said.

Against this tradition, some innovative judicial decisions have adopted a caveat, usually known as the "neutral

reportage" doctrine, permitting a responsible and neutral media outlet to print accusations made by one public figure or public organization against another, in the midst of a public controversy, without the media outlet itself being treated as "adopting the libel" as its own. The media outlet in such circumstances is in effect serving a public forum function, operating as a platform for the exchange of views. n273 This doctrine has obvious parallels to the "fair use" privilege in intellectual property, or the newsworthiness defense recognized in Bartnicki.

Similarly, American jurisdictions have long recognized the "fair reports" defamation privilege, granting immunity for neutral and balanced reporting of information taken from official proceedings. The privilege traces its lineage to early English cases. n274 The ancient fair reports privilege has its genesis in the notion that because members of the public have the right to attend judicial proceedings and observe them on their own, the media rightly should be permitted to serve as the "eyes and ears" of the public in reporting on those proceedings. In the words of Justice Oliver Wendell Holmes, "it is of vast public importance that the proceedings of courts of justice should be universally known," and it "is of the highest moment that those who administer justice should always act under the sense of public responsibility, and that every citizen should be able to satisfy himself with his own eyes as to the mode in which a public duty is performed." n275 Again, there are useful parallels. In privacy cases, we are highly unlikely to recognize a protected privacy interest in material presented in open court or garnered from public records. n276 In intellectual property law, there is a similar **[*1161]** resistance to granting copyright in government documents. n277

In sum, every detail of the "idea-expression" dichotomy or the fair use doctrine does not pose a freestanding question of First Amendment law. n278 But why not? The Copyright Clause and the First Amendment have peacefully coexisted for over 200 years. Fundamental to that coexistence is the presupposition that copyright protection does not impoverish the marketplace of ideas, but enriches it. n279 When a wrongdoer violates the copyright laws, the violation will virtually always involve some act of "expression." Indeed, the very paradigm of copyright violation, the wrongdoing infringer who copies a protected work without permission and sells the pirated copy in the market, is engaged in expressive activity. So too, the infringer who produces a "derivative work," such as a movie based on a novel, without obtaining the permission and license from the copyright owner of the underlying work, is engaged in "expression," perhaps highly creative and innovative expression, but that alone will not immunize the infringer from the reach of copyright law, including injunctive relief to enforce the limited monopoly of intellectual property ownership created by the Copyright Act. n280

[*1162] Bartnicki sits quite comfortably when juxtaposed with this intellectual property regime. Laws that protect privacy, like laws that protect intellectual property, may not be constitutionally "mandatory" in the sense that government is impelled to enact them, but they do reflect strong constitutional values (protection of privacy and protection of the works of authors and inventors both qualifying), and when constitutional "interests" are on both sides of the equation, some accommodating balance is appropriate. n281 The "newsworthiness" defense contemplated by the concurring and dissenting Justices, a defense that would not itself be independently subject to strict scrutiny, serves essentially the same function as "fair use" and the "idea-expression" dichotomy in copyright law. Moreover, when material is not "newsworthy," and thus outside exception now engrafted on statutes such as Title III (and long part of the common-law "private facts" tort), there is no special First Amendment impediment to prohibitions on trafficking in such material. In the intellectual property context, this is most powerfully represented by the long-standing rule that injunctions to enforce intellectual property rights are not unconstitutional prior restraints. To the contrary, prior restraints to protect intellectual property are commonplace. Injunctions to prevent theft of intellectual property exist as an incident to the character of the interest protected as property. n282 The First Amendment is not a license to trespass or to steal, and once violations of intellectual property rights have been established through the due process of adjudication, **[*1163]** courts may use their equitable powers to prevent such incursions. n283

The United States Court of Appeals for the Ninth Circuit, in the closely watched Napster litigation, recently sustained the granting of a preliminary injunction (with some modifications) against Napster, an online service that facilitated the unauthorized transfer of copyrighted musical recordings. n284 Napster was in some respects the ultimate antitrafficking case of the times, and in it the Ninth Circuit rejected a First Amendment "prior restraint" challenge to the injunction, targeted at Napster's contributory infringement activity, relying on the traditional understanding that prior

restraints to enforce rights in intellectual property do not offend the First Amendment. n285

That the outlines of the First Amendment's reconciliation with intellectual property law would fit so harmoniously with the matrix suggested for privacy by Bartnicki was perhaps in some way portended by the Supreme Court's decision in Zacchini v. Scripps-Howard Broadcasting Co., n286 a case that was nominally a privacy decision, but that in fact involved what is probably better understood as a species of intellectual property, a state-law "right of publicity" claim. The case involved the "human cannonball," Hugo Zacchini, and his act, which was getting shot from a cannon and flying 200 feet through the air into a net. Against his will and without his permission, a local television station filmed his performance at a county fair, and broadcast his entire act, which lasted about fifteen seconds, for **[*1164]** viewers. n287 The question before the Supreme Court was whether the First Amendment required the recognition of a "newsworthiness" privilege broad enough to immunize the television station for broadcasting Zacchini's performance. The Supreme Court held that no such First Amendment privilege existed specifically analogizing the state-created privacy-property right to federal intellectual property law, and noting that protection of the privacy-property right in such circumstances actually worked to foster and enhance First Amendment values, in much the same way that a majority of Justices in Bartnicki saw privacy protection as enhancing private speech. n288

None of this is meant to treat intellectual property as some kind of anti-First Amendment talisman capable of working a doughty voodoo guaranteed to keep the free speech doctor away. It is merely to say that the First Amendment cannot plausibly be understood to create anything approaching an absolute bar against information contraband, and that when contraband laws vindicating high social interests that are themselves of constitutional stature incorporate a structural balance sensitive to freedom of expression, such laws are constitutionally sustainable. It is, by all means, possible to overprotect intellectual property, by creating super-property regimes impervious to free speech defenses, regimes that ignore such fundamentals as the "idea-expression" dichotomy or fair use. As Judge Alex Kozinski once admonished:

Private property, including intellectual property, is essential to our way of life. It provides an incentive for investment and innovation; it stimulates the flourishing of our culture; it protects the moral entitlements of people to the fruits of their labors. But reducing too much to private property can be bad medicine. Private land, for instance, is far more useful if separated from other private land by public streets, roads and highways. Public parks, utility rights-of-way and sewers reduce the amount of land in private hands, but vastly enhance **[*1165]** the value of the property that remains.

So too it is with intellectual property. Overprotecting intellectual property is as harmful as underprotecting it. Creativity is impossible without a rich public domain. Nothing today, likely nothing since we tamed fire, is genuinely new: Culture, like science and technology, grows by accretion, each new creator building on the works of those who came before. Overprotection stifles the very creative forces it's supposed to nurture. n289

The ongoing case-by-case liquidation of this tension between overprotection and underprotection of intellectual property continues. In Comedy III Prods., Inc. v. Gary Saderup, Inc., n290 for example, the California Supreme Court recently applied California's statutory right of publicity to prevent exploitation of The Three Stooges comedy act, even though Moe Howard, Curly Howard, and Larry Fein, the stooges, were all dead. n291 The court held that neither the California statute's fair-use-style exemptions nor the First Amendment gave others the right to traffic in the personas of the Three Stooges without paying the freight. n292 We may imagine Moe, Curly, and Larry looking down from comedy heaven with delighted "whoop, **[*1166]** whoop, whoops," and "nyuck, nyuck, nyucks" at their posthumous litigation victory. Whether the Stooges and their progeny deserved to win or deserved to lose, the point is that California's law, existing at the intersection of privacy and property, contained doctrinal tools (such as fair use) sufficiently supple to properly focus the inquiry.

B. Official Secrets as Contraband

Late in President Clinton's presidency, Congress sent to the President an appropriations bill for America's intelligence operations that contained, for the first time in American history, an antitrafficking provision similar to the "Official Secrets Act" that has existed for some time in Great Britain. n293 President Clinton vetoed the bill, citing free speech concerns, and the chilling effect the law might have on public discourse, stating that "we must never forget that the free flow of information is essential to a democratic society." n294 The veto received widespread editorial praise. n295

The incident raised a fascinating question, however, particularly in light of the new legal intelligence generated by Bartnicki. Had the President chosen to sign the bill into law, would it have been unconstitutional? The bill as written did not appear to reach downstream disclosures of leaked classified information by the press, and so in that respect it created less a form of information contraband than Title III. As limited to government employees who leak classified material to the press, the bill might very well have been sustained against a First Amendment attack, for the Supreme Court has not heretofore recognized any First Amendment right of government employees to intentionally release classified information. To the contrary, the Supreme Court explicitly enforced such a limitation, imposing a constructive trust on the proceeds of a "kiss and tell" book written by a former CIA agent, n296 and at least one lower court has sustained criminal prosecutions against an intelligence agent who leaked material to the news media. n297

If Congress were to try again at an Official Secrets Act, and if a new **[*1167]** President signed it, could the new Congress and President attempt to go beyond what President Clinton vetoed, and impose liability on journalists for the mere receipt of the classified data, or for their subsequent disclosure of material illegally leaked to them by a government official? Parsing Bartnicki for answers, it is quite possible that a majority of the Justices would find room in the gradation of judgments for distinguishing between material leaked (intentionally or accidentally) by a government agent, in which the "crime" is the divulgence of government secrets by a government actor, and material taken from illegally intercepted private communications. n298 There is, arguably, a subtle but significant difference between a "steal" and a "leak." To borrow from basketball, these are two distinct kinds of turnovers. As a society, we are understandably in conflict over leaks. On the one hand, nobody loves the snitch, from childhood we are taught to ostracize the tattletale, and the ability to keep one's own counsel and another's confidences are generally regarded as honorable human traits. Yet one person's turncoat is another's whistleblower. In our private and public institutions we often depend on leaks to inform and enforce accountability. But a leak is not the same as a steal.

From the First Amendment perspective, a government leak is the government's problem. The government has the power to use its own devices to attempt to keep its secrets. But it may not use its monopoly on force to compel the press and the public to keep its secrets for it. n299 As Laurence Tribe has put it:

There may be some rough "law of the jungle" notion at work here: even if no sweeping right to know will be recognized as a limit on government's power to try to keep matters bottled up, an outsider who manages to obtain otherwise confidential information cannot then be prevented from disseminating it - or punished for having done so. n300

This creative and ongoing struggle between a vigilant press and the government is part of the genius of our constitutional system. The press is not entitled to a constitutional guarantee of success in this struggle, but it is entitled to a guarantee that when it does succeed, government will not inter **[*1168]** pose its sovereign power to penalize dissemination of the information it has obtained. In the words of Justice Potter Stewart:

So far as the Constitution goes, the autonomous press may publish what it knows, and may seek to learn what it can.

But this autonomy cuts both ways. The press is free to do battle against secrecy ... . but the press cannot expect from the Constitution any guarantee that it will succeed. n301

Journalists may not demand success in uncovering the truth. They may demand the right to publish what they succeed in uncovering. If the government wants to protect itself against leaks, it must do what it can to plug its own holes. n302 But it may not adopt the simple expedient of penalizing the press for using the material given to it. n303

Respect for the structural independence of the media contemplated by the Constitution prohibits courts from conscripting journalists as leak-police. n304 A bright line is required here. The journalist cannot be forced to **[*1169]** ask the government source who hands her the document: "Are you sure this is legal? Are you sure this is not under seal?" The bright line is simple and easy to enforce: If the journalist steals information by breaking the law to obtain it, the journalist is subject to whatever generally applicable legal penalties may apply. If the journalist is handed information, the journalist may examine it and publish it. The journalist is protected whether or not the material is labeled "confidential," "classified," or "filed under seal; to be opened only by the court." The journalist is protected whether the information is in a typed document, on a cassette tape, or a computer diskette. The journalist is protected whether the material is or is not in an envelope, sealed or unsealed. The press and the government are thus locked in contest. The press's "chief responsibility is to play its role in that contest, for it is the contest that serves the public interest, which is not wholly identified either with the interest of the government of the day, or of the press." n305

When the government is not the "opponent" in the contest, however, the calculus significantly changes. When an official secret is disclosed, no one's constitutional privacy rights are typically violated, because the government as a government has no cognizable constitutional privacy rights, in much the same sense that the government has no "reputation" that can be vindicated in a government cause of action for libel. n306 When a private in **[*1170]** dividual's privacy rights are trammeled, however, there is a violation of a personal right of constitutional dimension, as all of the Justices in Bartnicki accepted, n307 and in this posture a law calculated to vindicate those interests, provided it contains the type of newsworthiness safety valve Bartnicki contemplated, is on a different constitutional footing. n308

C. Criminal and Tortious Contraband

There is a growing societal interest in the imposition of criminal and civil liability for trafficking in information intended to facilitate the violation of law. The legal and policy issues posed by this emerging form of information contraband are vast and complex, and alas, beyond the length limits of this enterprise. The problem is worth noting very briefly, however, as yet one more foil on the implications of Bartnicki. Two relatively recent cases illustrate the range of instances in which society might be tempted to impose liability for such contraband: one, Rice v. Paladin Enterprises, Inc., n309 involving the publication of an instruction manual providing technical assistance on how to perpetrate murder-for-hire; the other, Universal **[*1171]** City Studios, Inc. v. Corley, n310 involving the enforcement of a federal law making it illegal to traffic in devices marketed for the purpose of defeating encryption devices protecting copyrighted works. In Rice, the United States Court of Appeals for the Fourth Circuit held that a viable cause of action in tort for aiding and abetting murder existed against the publisher of a murder manual entitled Hit Man: A Technical Manual for Independent Contractors, which was allegedly used by a professional hit man as the blueprint for three murders. n311 The book publisher defendant in Rice relied heavily on the Daily Mail line of cases, arguing that all of the information contained in the Hit Man manual was "truthful," and thus constitutionally protected, unless the plaintiffs could meet the highly demanding standard currently applicable in incitement cases, n312 as articulated in the Supreme Court's landmark decision in Brandenburg v. Ohio. n313 In Brandenburg the Supreme Court held that the constitutional guarantees of free speech and free press do not permit a state to forbid or proscribe advocacy of the use of force or of law violation except where such advocacy is directed to inciting or producing imminent lawless action and is likely to incite or produce such action. n314

In Universal, the defendants challenged the constitutionality of the Digital Millennium Copyright Act of 1998

("DMCA"). n315 Movie studios today usually "encrypt" films distributed in DVD (digital versatile disk) format, so they cannot be copied and pirated, using a "contents scramble system" ("CSS"). n316 What can be scrambled can usually be descrambled, however, and soon the scrambled DVDs were under assault from technologies designed to descramble them, appropriately called "De-CSS." Congress, in passing the DMCA, weighed in on these technology wars, passing provisions prohibiting trafficking in devices intended to circumvent encryption and scrambling technologies placed in copyrighted works by copyright holders to protect their works from unauthorized copying. n317 As in Rice and **[*1172]** Bartnicki, the defendants in Universal relied on the Daily Mail line of cases, arguing that the anti-encryption software they marketed was "true" information that could not be proscribed under the First Amendment.

The problems posed by these kind of criminal and tortious contraband cases go well beyond the issues posed by the antitrafficking laws at issue in Bartnicki, but even so, the holding in Bartnicki must now be incorporated as part of the conversation. If at least five, and perhaps as many as nine Justices in Bartnicki did not find the Daily Mail principle so imposing that it would automatically render unconstitutional laws prohibiting trafficking in privacy contraband, it is likely that a majority of Justices would find that, at least in some circumstances, laws forbidding trafficking in information intended to facilitate murder, or wholesale pirating of intellectual property, could be similarly upheld.

More pointedly, Bartnicki made "newsworthiness" the mediating line between proscribable contraband and protected public discourse. The Rice case adopted a similar division, and so did Congress in passing the DMCA. In Rice, the holding of the Court of Appeals that the Hit Man manual was not absolutely protected by the First Amendment was grounded largely in its view that there was no "abstract advocacy" or "political discourse" in the detailed how-to instructions contained in the murder manual. The book at issue was essentially exhortation and detailed factual information on how to go into business as a paid assassin and carry out executions. Hit Man was not a political manifesto, an outpouring of conscience, or credo. It was instruction and encouragement in the dark arts of mercenary murder. n318 The defendants in Rice stipulated (for purposes of a motion for summary judgment and the ensuing appeal) that they knew and intended that the murder manual would be used by real criminals to plan and execute murders. The Court of Appeals in Rice held that

Paladin's astonishing stipulations, coupled with the extraordinary comprehensiveness, detail, and clarity of Hit Man's instructions for criminal activity and murder in particular, the boldness of its palpable exhortation to murder, the alarming power and effectiveness of its peculiar form of instruction, the notable absence from its text of the kind of ideas for the protection of which the First Amendment exists, and the book's evident lack of any even arguably legitimate purpose beyond the promotion and teaching of murder, render this **[*1173]** case unique in the law. In at least these circumstances, we are confident that the First Amendment does not erect the absolute bar to the imposition of civil liability for which Paladin Press and amici contend. n319

Bartnicki seems entirely consistent with this holding, for one can easily fit the result in Rice to the framework of Bartnicki, treating the social judgment not to permit deliberate and intentional instruction in murder as an interest sufficiently "important" or "compelling" to satisfy any plausible "macro" First Amendment standard, and certainly as important as the protection of privacy.

Similarly, Bartnicki does not impugn the constitutional validity of the DMCA at issue in Universal. The wholesale copying of a movie in contravention of the rights of the copyright holders is by no stretch a "fair use," and this was not the defense in Universal. Rather, the somewhat more exotic claim was made that some people might make use of De-CSS technology to assist them in making "fair use" of a copyrighted movie. The examples offered were professors or students who wish to copy small snippets from movies and compile them on one disk for the purposes of illustrating a film lecture, a movie reviewer who wants to quote or copy a portion of a film as part of a review, a television station or news program seeking to show some portion of a review during a broadcast discussing or critiquing a movie. These are good examples because they all fall within the classic paradigms of "fair users" - academics, students, reviewers, or journalists who seek to reproduce limited portions of a copyrighted work in order to critique or comment upon it.

The problem with these examples is that it is difficult to see how, in any meaningful sense, the DMCA interfered with the rights of such fair users. Nothing in copyright law requires a copyright holder to make it easy to copy works. While the law permits fair use, it imposes no affirmative obligation on the author to facilitate it. So too, nothing in the law prohibits copyright owners from making it difficult to copy works, so as to discourage pirating. The owners of copyrighted movies, for example, frequently distribute their films on a pay-per-view basis, via cable television or satellite networks, in which the movies are electronically scrambled to prevent unauthorized viewing. Ingenious bandits nevertheless at times traffic in devices marketed solely to permit users to steal the movies from the cable or satellite distribution systems. Courts have properly treated such "expression" as nothing more than an incident to larceny, and not immunized by the First Amendment. n320 When Congress was confronted with evidence of **[*1174]** new technological developments that threatened the integrity of traditional copyright protection, Congress was entitled to enact additional kinds of legal protection to respond to the threat, lest copyright protection of digital works be rendered a legal fiction. n321 While the tension between the system of copyright protection and the system of free expression may not have the mathematical rigidity of a zero-sum game, it nevertheless largely remains that society cannot have it both ways. We cannot maintain a meaningful regime of intellectual property protection if the property right may be nullified by anyone who may plausibly assert a free speech right to disseminate "truthful information."

There may, of course, be some value in de-encryption technology in and of itself, value that can be separated from its use as a tool to invade copyright interests. Bartnicki would seem to require congressional sensitivity to this, analogous to the "fair use" or "newsworthiness" defenses. But Congress was aware of this, and took pains to carve out exceptions from the DMCA that would cover virtually all plausible examples of such value. Indeed, the DMCA is well calculated to protect the benign use of de-encryption technology, for the law is narrowed both by negation and affirmation. The law only purports to reach devices marketed for infringing purposes. As an extra measure of protection, however, Congress carefully catalogued the principal legitimate uses that it could envision, and on top of the law's negative limitation, explicitly immunized such uses through various affirmative defenses listed in the statute, to the extent that it was possible to do that without unduly endangering digital copyrighted, technologically protected works generally. n322

Finally, as much as Bartnicki invites balancing when interests of constitutional dimension exist on both sides of the equation, n323 the constitutional equities in the case of the DMCA are overwhelmingly one-sided. On one side of the balance is a technology that exists almost exclusively to subvert copyright protection. n324 On the other side of the scale are highly speculative hypothetical uses in which the unavailability of the technology might make the copying of a copyrighted work for fair use purposes marginally more inconvenient. n325 In the small range of cases where a legitimate **[*1175]** fair user is slightly inconvenienced, that inconvenience is a social cost well worth the benefit it achieves in deterrence of piracy, and certainly well within the balance that Congress was entitled to strike. Lastly, in both Rice and Universal, the defendants sounded themes of civil disobedience, as if the very act of trafficking in the unprotected was itself a statement that rendered the trafficking protected. Lawlessness for its own sake thus becomes constitutionally sacrosanct because it is nihilism, itself a philosophy. This argument, however, conflates motive with intent. An individual may intentionally commit murder for what the individual perceives as altruistic motives (as in the case of a terrorist murdering out of religious conviction), but this does not render the act beyond the punishment of the law. More fundamentally, whatever moral sensibilities may compel a person to break the law as a gesture of protest, the breaking of the law is not thereby excused. Civil disobedience in its classic form is undertaken with an expectation that punishment will follow. n326

Conclusion

It is perhaps fitting that this exploration of information as contraband should have ended with the short reminder that the nihilistic thrill of civil disobedience, whether it be scanning to eavesdrop on a private conversation, training in murder-for-hire, or marketing software to pirate movies, is not entitled to any profound respect. Self-proclaimed status as a civil disobedient is not enough to infuse one's actions with any deep moral resonance. Cell-phone scanning, murder-manual publishing, and digital hacking are hardly the stuff of Martin Luther King, Jr., Mahatma Ghandi, or

Henry David Thoreau. Nor are laws that seek to deter trafficking in the contraband of such antisocial acts laws passed out of the sinister censorial motives that offend the core of the First Amendment. As a majority of the Justices in Bartnicki acknowledged, balanced measures are called for, and sometimes there is room in our constitutional system for a measure of balance.

Legal Topics:

For related research and practice materials, see the following legal topics:
Constitutional LawBill of RightsFundamental FreedomsFreedom of SpeechForumsConstitutional LawBill of RightsFundamental FreedomsFreedom of SpeechObscenityCriminal Law & ProcedureCriminal OffensesMiscellaneous OffensesIllegal EavesdroppingElements

FOOTNOTES:

n1. 532 U.S. 514 (2001).

n2. 18 U.S.C. 921-928, 2510-2520, 3101, 3502 (2000).

n3. 18 U.S.C. 2511 (2000). Title III of the Omnibus Crime Control and Safe Streets Act of 1968, as amended by the Electronic Communications Privacy Act of 1986, provides in pertinent part that it is a violation of law when any person:

(c) intentionally discloses, or endeavors to disclose, to any other person the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection; [or]

(d) intentionally uses, or endeavors to use, the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection.

Id.

n4. 18 U.S.C. 2520(a)-(c) (2000). In such a suit, the plaintiff may obtain equitable or declaratory relief, damages (calculated as the greater of actual damages or specified statutory damages), punitive damages, and attorney's fees and costs. 18 U.S.C. 2520(b)-(c).

n5. Depending on exactly what statutes one counts, as many as 44 states prohibited interception and disclosure of electronic communications in some circumstances, in statutory provisions that are often patterned closely after Title III. See, e.g., Ala. Code 13A-11-31, 13A-11-35 (1994); Alaska Stat. 42.20.300-42.20.330 (Michie 1989 & Supp. 1995); Ariz. Rev. Stat. Ann. 13-3005, 13-3006 (West 1989); Cal. Penal Code 631, 632 (West 1999); Colo. Rev. Stat. 18-9-303 (1986 & Supp. 1995); Conn. Gen. Stat. 53a-187, 53a-188, 53a-189, 54-41r (1994); Del. Code Ann. tit. 11, 1336 (1996); Ga. Code Ann. 16-11-62, 16-11-66.1 (1994); Haw. Rev. Stat. 803-42 (1995); Idaho Code 18-6702 (Michie 1996); 720 Ill. Comp. Stat. Ann. 5/14-2 (West 1993); Ind. Code Ann. 35-45-2-4 (West 1994); Iowa Code Ann. 808B.2, 808B.8 (West 1994); Kan. Stat. Ann. 21-4002 (1996); Ky. Rev. Stat. Ann. 526.020, 526.060 (Michie 1998); La. Rev. Stat. Ann. 15:1303, 15:1312 (West 1992); Me. Rev. Stat. Ann. tit. 15, 710, 711 (West 1998); Md. Code Ann., Cts. & Jud. Proc. 10-402 (1998); Mass. Gen. Laws Ann. ch. 272, 99(c) (West 1990); Mich. Comp. Laws Ann. 750.539c, 750.539e, 750.539h (West 1991 & Supp. 1995); Minn. Stat. Ann. 626A.02, 626A.13 (West 1998); Mo. Rev. Stat. 542.402, 542.418 (1996); Mont. Code Ann. 45-8-10 (1997); Neb. Rev. Stat. 86-702, 86-707.02 (1995); Nev. Rev. Stat. 200.620, 200.630, 200.650, 200.690 (1994); N.H. Rev. Stat. Ann. 570-A:2 (1995); N.J. Stat. Ann. 2A-156A-3, 2A-156A-24 (West 1985 & Supp. 1999); N.M. Stat. Ann. 30-12-14, 30-12-11 (Michie 1994); N.Y. Penal Law 250.05, 250.25 (McKinney 1989 & Supp. 1995); N.C. Gen. Stat. 15A-287 (1996); N.D. Cent. Code 12.1-15-02 (1994); Ohio Rev. Code Ann. 2933.52, 2933.65 (West 1998); Okla. Stat. Ann. tit. 13, 176.2 to 176.5 (West 1994); Or. Rev. Stat. 165.540, 165.543 (1998); 18 Pa. Cons. Stat. Ann. 5703, 5725 (West 1999); R.I. Gen. Laws 11-35-21 (1998); Tenn. Code Ann. 39-13-601 to 39-13-603 (1994); Tex. Penal Code Ann. 16.02, 16.05 (Vernon 1994); Utah Code Ann. 77-23a-4, 77-23a-11 (1994); Va. Code Ann. 19.2-62, 19.2-69 (Michie 1990); W. Va. Code 62-1D-3, 62-1D-12 (1990); Wis. Stat. Ann. 968.31 (West 1985 & Supp. 1999); Wyo. Stat. 7-3-602, 7-3-611 (1987); see also Ark. Code Ann. 5-60-120(a) (Michie 1994) (while not directly prohibiting subsequent disclosure, statute does make it a crime to "record or possess a recording of such communication"); D.C. Code Ann. 23-542, 23-554 (1996).

n6. See Pennsylvania Wiretapping and Electronic Surveillance Control Act, 18 Pa. Cons. Stat. Ann. 5703(2)-(3) (West 1999) (making it a felony when any person "intentionally discloses or endeavors to disclose to any other person the contents of any wire, electronic or oral communication, or evidence derived therefrom, knowing or having reason to know that the information was obtained through the interception of a wire, electronic or oral communication," or "intentionally uses or endeavors to use the contents of any wire, electronic or oral communication, or evidence derived therefrom, knowing or having reason to know, that the information was obtained through the interception of a wire, electronic or oral communication").

n7. See Bartnicki v. Vopper, 532 U.S. 514, 541 (2001) (Breyer, J., concurring) (noting that, while cell phone users tolerate casual eavesdropping on their ordinary conversations on the street, technologies now exist that allow eavesdropping on encrypted cell phone conversations, or on conversations that take place in the home).

n8. S. Rep. No. 90-1097, at 67 (1968).

n9. Id.

n10. Id.

n11. When Senator Patrick Leahy opened the Senate hearings in 1984 on "the electronic revolution" and its impact "on our lives and our sense of privacy," he noted that we now send electronically everything from "sophisticated legal documents," to "a bid," to "a love letter." Oversight on Communications Privacy: Hearing Before the Subcomm. on Patents, Copyrights and Trademarks of the Comm. on the Judiciary United States Senate, 98th Cong. 1-2 (1984) (statement of Sen. Leahy). What we now know, of course, was that by today's standards, Congress, in 1984, hadn't seen nothin' yet.

n12. See Electronic Communications Privacy Act: Hearings Before the Subcomm. on Courts, Civil Liberties, and the Administration of Justice, Senate Committee on the Judiciary, 99th Cong. 2 (1986). Congress found that "tremendous advances in telecommunications and computer technologies have carried with them comparable technological advances in surveillance devices and techniques," such that private information "may be open to possible wrongful use and public disclosure by ... unauthorized private parties." S. Rep. No. 99-541, at 3 (1986). Congress thus saw the need for "statutory standards to protect the privacy and security of communications transmitted by new noncommon carrier communications services or new forms of telecommunications and computer technology," which "American citizens and American businesses are using ... in lieu of, or side-by-side with, first-class mail and common carrier telephone services." Id. at 5; see also United States v. United States Dist. Ct., 407 U.S. 297, 302 (1972) ("[Title III] represents a comprehensive attempt by Congress to promote more effective control of crime while protecting the privacy of individual thought and expression.").

n13. S. Rep. No. 99-541, at 18 (1986).

Since Congress last addressed the issue of privacy communications in a comprehensive fashion, the technologies of communication and interception have changed dramatically, and are expected to continue to do so. These factors have raised serious issues about the protection of the privacy interests of U.S. citizens, which are of great concern to the Senate and the American people.

Id.

n14. See 18 U.S.C. 2511(2)(d) (2000). This is the norm in most, but not all states.

n15. 47 U.S.C. 302a(d) (2000). The statute, passed in 1993, makes it illegal to manufacture scanners that can intercept cellular transmissions.

n16. See Kimberly R. Thompson, Cell Phone Snooping: Why Electronic Eavesdropping Goes Unpunished, 35 Am. Crim. L. Rev. 137, 151 (1997).

n17. Id. at 149 (citing estimate that between 10 and 20 million scanners are currently in use in the United States); see also Bartnicki v. Vopper, 532 U.S. 514, 549 (2001) (Rehnquist, C.J., dissenting) ("It is estimated that over 20 million scanners capable of intercepting cellular transmissions currently are in operation ... notwithstanding the fact that Congress prohibited the marketing of such devices eight years ago." (citation omitted)).

n18. See, e.g., Nalley v. Nalley, 53 F.3d 649 (4th Cir. 1995) (ex-wife sued by ex-husband, who had been having an affair, when a tape recording revealing the affair was sent to the wife anonymously by a third party, and the wife played the recording for the couple's children, the husband of the woman with whom her husband was having the extramarital affair, and her attorney); Kempf v. Kempf, 868 F.2d 970 (8th Cir. 1989) (ex-wife who had allegedly had several extramarital affairs sued her ex-husband for his recording of phone conversations between the ex-wife and her alleged paramours); Lizza v. Lizza, 631 F. Supp. 529 (E.D.N.Y. 1986) (ex-husband sued by ex-wife when he recorded calls made by her from their home phone for use in a divorce proceeding); Kratz v. Kratz, 477 F. Supp. 463 (E.D. Pa. 1979) (ex-wife and her lover sued wife's ex-husband and his lawyer when the husband secretly recorded phone conversations between them on the house telephone for the purposes of gathering evidence of their affair, when the contents of the tapes were used in a divorce proceeding).

n19. See, e.g., Pollock v. Pollock, 154 F.3d 601 (6th Cir. 1998) (ex-wife secretly recorded telephone conversations between her ex-husband and their minor daughter during a child-custody dispute and made subsequent disclosures and use of the recordings); Scheib v. Grant, 22 F.3d 149 (7th Cir. 1994) (ex-wife sued the lawyers of her ex-husband, after the husband recorded her phone calls with their son, and gave them to his lawyers, who then attempted to make use of them in a child custody hearing); Kirkland v. Franco, 92 F. Supp. 2d 578 (E.D. La. 2000) (ex-wife sued her ex-husband who secretly recorded phone conversations after suspicions that his wife had been unfaithful, and then disclosed contents to wife's mother, boss, and pastor, and then used the contents during a child-custody hearing); Thompson v. Dulaney, 838 F. Supp. 1535 (D. Utah 1993) (ex-wife taped her ex-husband's phone conversations with their children and disclosed contents to lawyers, parents, and expert witnesses during divorce proceedings); Janecka v. Franklin, 684 F. Supp. 24 (S.D.N.Y. 1987) (ex-husband sued by ex-wife for recording telephone conversations between ex-wife and their minor children).

n20. See, e.g., Newcomb v. Ingle, 944 F.2d 1534 (10th Cir. 1991) (a child sued his mother because the mother secretly recorded a telephone conversation in which the child's father gave the child instructions as he set fire to the family home).

n21. See, e.g., Chandler v. United States Army, 125 F.3d 1296 (9th Cir. 1997) (an Army Captain sued the Army when illegally intercepted phone conversations made by his wife were used by the Army in an adultery investigation); Bast v. Cohen, Dunn & Sinclair, P.C., 59 F.3d 492 (4th Cir. 1995) (suit arising from secretly recorded phone conversations during dissolution of extramarital affair); Deal v. Spears, 980 F.2d 1153 (8th Cir. 1992) (plaintiff's phone conversations secretly recorded by his employer, who had done the tapping to investigate suspicions of employee robbery, but who discovered instead that the plaintiff was having an extramarital affair, which the employer then disclosed); Fultz v. Gilliam, 942 F.2d 396 (6th Cir. 1991) (ex-wife brought suit against her ex-husband for surreptitiously tape-recording her phone conversations with her boyfriend and playing them for her daughter, brother, and pastor); Pritchard v. Pritchard, 732 F.2d 372 (4th Cir. 1984) (ex-wife was sued by ex-husband when she bugged the home phone and made secret recordings of his phone calls); United States v. Jones, 580 F.2d 219 (6th Cir. 1978) (ex-husband prosecuted for the illegal interception and use of phone calls of his estranged wife).

n22. See, e.g., Boehner v. McDermott, 191 F.3d 463 (D.C. Cir. 1999) (Republican congressman sued Democratic congressman when a Florida couple, using a mobile police scanner while tailing the plaintiff's car, recorded a cellular telephone call containing politically damaging information and gave copies of the tape to defendant, who in turn released it to the press); United States v. Newman, 476 F.2d 733 (3d Cir. 1973) (a member of a city council induced an employee of the phone company to illegally intercept and record phone conversations of political opponents to obtain information that would be politically damaging to them).

n23. See, e.g., Asmar v. Detroit News, Inc., 836 F.2d 1347 (6th Cir. 1988) (anonymously recorded call of conversation revealing bribery by competing contractor sent to newspaper and government contractor).

n24. See, e.g., Weeks v. Union Camp Corp., 215 F.3d 1323 (4th Cir. 2000) (employees sued employer for conversations surreptitiously recorded in the workplace and used to discipline or dismiss employees); Desilets v. Wal-Mart Stores, Inc., 171 F.3d 711 (1st Cir. 1999) (Wal-Mart employees sued Wal-Mart for alleged secret recordings of phone conversations made during the night shift); Epps v. St. Mary's Hosp. of Athens, Inc., 802 F.2d 412 (11th Cir. 1986) (emergency medical workers sued the hospital they worked for and certain coworkers after secretly recorded phone conversations were disclosed and used); Spetalieri v. Kavanaugh, 36 F. Supp. 2d 92 (N.D.N.Y. 1998) (employee, a police administrator, sued when a scanner was used to record conversations from his home and used as part of a work investigation and disciplinary proceeding against him); Dorris v. Absher, 959 F. Supp. 813 (M.D. Tenn. 1997) (employees sued when a supervisor secretly recorded personal phone conversations made from office phones and then attempted to make use of those conversations to terminate the employees); Wesley Coll. v. Pitts, 974 F. Supp. 375 (D. Del. 1997) (college president sent e-mails,

which were copied on hard copies and distributed in unmarked envelopes; the college sued faculty members and a clerical employee for distributing the contents of the e-mails).

n25. Even crooks have feelings. See, e.g., Freeman v. Ramada Inn, Inc., 805 F.2d 1034 (6th Cir. 1986) (a convicted robber sued the police and the Ramada Inn hotel chain after the hotel rerouted a call placed by the robber to his accomplice, who was a guest at a Ramada Inn, to the police, who later used the contents of the call to prosecute the robber).

n26. See, e.g., Berry v. Funk, 146 F.3d 1003 (D.C. Cir. 1998) (Ex-Acting Assistant Secretary of State sued State Department officials for monitoring phone calls, using and disclosing the contents of the calls during the President Clinton White House passport scandal investigation); Rodgers v. Wood, 910 F.2d 444 (7th Cir. 1990) (police officers sued a suspect, who secretly recorded phone calls, made by the police officers from the suspect's home, that were disclosed to other officers and a prosecutor, and used by the suspect's attorney in court).

n27. See, e.g., Peavy v. WFAA-TV, Inc., 221 F.3d 158 (5th Cir. 2000) (a person involved in numerous disputes with his neighbor surreptitiously intercepted and tape recorded the neighbor's phone conversations, and then turned the tapes over to a local television station); Davis v. Zirkelbach, 149 F.3d 614 (7th Cir. 1998) (the plaintiff's employer secretly recorded the plaintiff's phone conversations and the recordings were disclosed to police and city officials who used contents to persuade a witness to cooperate in an investigation of the plaintiff's alleged narcotics trafficking); Forsyth v. Barr, 19 F.3d 1527 (5th Cir. 1994) (police officers who were under investigation by an internal affairs unit sued for the secret interception of conversations the officers had with an informant, when the calls were intercepted by the informant's neighbors).

n28. Cal. Civ. Code 1708.8 (West 1998).

n29. California law states as follows:

A person is liable for physical invasion of privacy when the defendant knowingly enters onto the land of another without permission or otherwise committed a trespass, in order to physically invade the privacy of the plaintiff with the intent to capture any type of visual image, sound recording, or other physical impression of the plaintiff engaging in a personal or familial activity and the physical invasion occurs in a manner that is offensive to a reasonable person.

Cal. Civ. Code 1708.8(a).

n30. California law states as follows:

A person is liable for constructive invasion of privacy when the defendant attempts to capture, in a manner that is offensive to a reasonable person, any type of visual image, sound recording, or other physical impression of the plaintiff engaging in a personal or familial activity under circumstances in which the plaintiff had a reasonable expectation of privacy, through the use of a visual or auditory enhancing device, regardless of whether there is a physical trespass, if this image, sound recording, or other physical impression could not have been achieved without a trespass unless the visual or auditory enhancing device was used.

Cal. Civ. Code 1708.8(b).

n31. California law states as follows:

For the purposes of this section, "personal and familial activity" includes, but is not limited to, intimate details of the plaintiff's personal life, interactions with the plaintiff's family or significant others, or other aspects of plaintiff's private affairs or concerns. Personal and familial activity does not include illegal or otherwise criminal activity as delineated in subdivision (f). However, "personal and familial activity" shall include the activities of victims of crime in circumstances where either subdivision (a) or (b), or both, would apply.

Cal. Civ. Code 1708.8(k).

n32. California law states as follows:

For the purposes of this section, "personal and familial activity" includes, but is not limited to, intimate details of the plaintiff's personal life, interactions with the plaintiff's family or significant others, or other aspects of plaintiff's private affairs or concerns. Personal and familial activity does not include illegal or otherwise criminal activity as delineated in subdivision (f). However, "personal and familial activity" shall include the activities of victims of crime in circumstances where either subdivision (a) or (b), or both, would apply.

Cal. Civ. Code 1708.8(k). In Bartnicki, the critical "swing" votes of two Justices, Breyer and O'Connor, seemed to turn on their perception that the intercepted conversations discussed possible violent criminal activity. Bartnicki v. Vopper, 532 U.S. 514, 539 (2001) (Breyer, J., concurring); see infra text accompanying notes 55-62.

n33. California law states as follows:

For the purposes of this section, "for a commercial purpose" means any act done with the expectation of a sale, financial gain, or other consideration. A visual image, sound recording, or other physical impression shall not be found to have been, or intended to have been captured for a commercial purpose unless it is intended to be, or was in fact, sold, published, or transmitted.

Cal. Civ. Code 1708.8(j). The California law authorizes civil actions for damages (including punitive damages and treble damages), for the disgorgement of profits from the sale of the information and equitable relief against future violations. Cal. Civ. Code 1708.8(c).

n34. Cal. Civ. Code 1708.8(d).

n35. Cal. Civ. Code 1708.8(e).

Sale, transmission, publication, broadcast, or use of any image or recording of the type, or under the circumstances, described in this section shall not itself constitute a violation of this section, nor shall this section be construed to limit all other rights or remedies of plaintiff in law or equity, including, but not limited to, the publication of private facts.

Id.

n36. A bill introduced in the United States House of Representatives in 1998, H.R. 3224, prohibited certain stalking tactics done to obtain "a visual image, sound recording, or other physical impression of that or another individual," for the purposes of commercial sale in situations in which the individual has "has a reasonable expectation of privacy from such intrusions and has taken reasonable steps to ensure that privacy," when the "individual has a reasonable fear that death or bodily injury will result from that following or chasing." Privacy Protection Act of 1998, H.R. 3224, 105th Cong. 1822 (1998).

n37. This proposal thus reached the use of high-powered lenses, microphones, or even helicopters to trespass for commercial purposes, forbidding the use of visual or auditory enhancement devices to capture recordings that one otherwise could not have captured without trespassing.

n38. Four categories of common-law actions for invasion of privacy are generally recognized in the United States, though not all jurisdictions acknowledge all of them, and their elements vary slightly from state to state. See generally Rodney Smolla, Law of Defamation 10:1, 10:2, at 10-1-10-4 (2d ed. 2000). The four actions are "false light" invasion of privacy, a tort parallel in many respects to defamation, see Cantrell v. Forest City Publ'g

Co., 419 U.S. 245 (1974); Time, Inc. v. Hill, 385 U.S. 374 (1967); "intrusion," a tort that involves invasion of a plaintiff's private space or solitude, see Gallella v. Onassis, 487 F.2d 986 (1973); "publication of private facts," a cause of action for public disclosure of a private fact which would be offensive and objectionable to the reasonable person and which is not of legitimate public concern, see Michaels v. Internet Entm't Group, Inc., 5 F. Supp. 2d 823, 841-42 (C.D. Cal. 1998); Diaz v. Oakland Tribune, Inc., 188 Cal. Rptr. 762, 768 (Cal. Ct. App. 1983); and "appropriation of name or likeness" (or invasion of the "right of publicity"), a cause of action for the unauthorized use of a persons name or likeness (in most jurisdictions, for commercial purposes). See Rodney A. Smolla, Free Speech in an Open Society 117-50 (1992) [hereinafter Smolla, Free Speech]; Randall Bezanson, The Right to Privacy Revisited: Privacy, News, and Social Change: 1890-1990, 74 Cal. L. Rev. 789 (1986); Diane Zimmerman, Requiem for a Heavyweight: A Farewell to Warren and Brandeis's Privacy Tort, 68 Cornell L. Rev. 291 (1983). The "false light" tort is not particularly germane to this Article, and is not discussed. "Intrusion" and "publication of private facts" are examined here; "appropriation," which is probably better understood as a species of intellectual property in one's own identity and persona, is discussed later, in the context of intellectual property. See infra text accompanying notes 262-279.

n39. See Restatement (Second) of Torts 652B (1977).

n40. As the court stated in McNally v. Pulitzer Publishing Co.:

Although the manner in which information is obtained may be relevant in assessing whether the privacy tort of intrusion has been committed, the law in this developing area seems to be that a newspaper does not commit intrusion by its mere receipt of tortiously obtained private facts, even when the newspaper has actual knowledge of such impropriety.

532 F.2d 69, 79 n.14 (8th Cir. 1976); see Pearson v. Dodd, 410 F.2d 701, 703-05 (D.C. Cir. 1969) (refusing to permit a common-law intrusion claim against journalists who had received and published the contents of documents stolen from a United States Senator's office by third parties).

n41. See, e.g., Michaels v. Internet Entm't Group, Inc., 5 F. Supp. 2d 823, 841-42 (C.D. Cal. 1998); Diaz v. Oakland Tribune, Inc., 188 Cal. Rptr. 762, 768 (Cal. Ct. App. 1983); Briscoe v. Reader's Digest Ass'n, 93 Cal. Rptr. 866 (Cal. Ct. App. 1971).

n42. See Smolla, Free Speech, supra note 38, at 132-41.

n43. This includes grappling with such problems as whether one may "regain" one's privacy after exposure in some public event through the passage of time. As the court stated in Briscoe v. Reader's Digest Ass'n:

We are realistic enough to recognize that men are curious about the inner sanctums of their neighbors - that the public will create its heroes and villains. We must also be realistic enough to realize that full disclosure of one's inner thoughts, intimate personal characteristics, and past life is neither the rule nor the norm in these United States. We have developed a variegated panoply of professional listeners to whom we confidentially "reveal all"; otherwise we keep our own counsel. The masks we wear may be stripped away upon the occurrence of some event of public interest. However, just as the risk of exposure is a concomitant of urban life, so too is the expectation of anonymity regained. It would be a crass legal fiction to assert that a matter once public never becomes private again.

483 P.2d 34, 41 (Cal. 1971).

n44. See Smolla, Free speech, supra note 38, at 132-41.

n45. See generally Robert Post, The Social Foundations of Privacy: Community and Self in the Common Law Tort, 77 Cal. L. Rev. 957, 1007 (1989) (observing that the newsworthiness test "bears an enormous social pressure, and it is not surprising to find that the common law is deeply confused and ambivalent about its application").

n46. As the court stated in Diaz v. Oakland Tribune, Inc.:

The proof that defendants have published an article containing highly offensive private matters does not itself establish a claim for relief. It certainly must be recognized that an otherwise embarrassing article may be newsworthy, depending on the circumstances. Only when the embarrassing publicity is not newsworthy can plaintiff recover damages, consistent with defendants' rights of free speech and press.

188 Cal. Rptr. 762, 770 (Cal. Ct. App. 1983); see Neff v. Time, Inc., 406 F. Supp. 858, 861 (W.D. Pa. 1976) (stating that a "factually accurate public disclosure is not tortious when connected with a newsworthy event even though offensive to ordinary sensibilities").

n47. See, e.g., Florida Star v. B.J.F., 491 U.S. 524 (1989); Haynes v. Knopf, Inc., 8 F.3d 1222 (7th Cir. 1993); Ross v. Midwest Communications, Inc., 870 F.2d 271 (5th Cir. 1989); Gilbert v. Med. Econ. Co., 665 F.2d 305 (10th Cir. 1981); Campbell v. Seabury Press, 614 F.2d 395 (5th Cir. 1980); Pasadena Star-News v. Superior Ct., 203 Cal. App. 3d 131 (Cal. Ct. App. 1988); Sipple v. Chronicle Publ'g Co., 201 Cal. Rptr. 665 (Cal. Ct. App. 1984); McNutt v. N.M. State Tribune Co., 538 P.2d 804 (N.M. Ct. App. 1975); Freihofer v. Hearst Corp., 480 N.E.2d 349 (N.Y. 1985); Anderson v. Fisher Broad. Co., 712 P.2d 803 (Or. 1986).

n48. See Harry Kalven, Privacy in Tort Law - Were Warren and Brandeis Wrong?, 31 Law & Contemp. Probs. 326 (1966).

n49. For instance, in Diaz v. Oakland Tribune, Inc., the court stated:

In an effort to reconcile these competing interests, our courts have settled on a three-part test for determining whether matter published is newsworthy: "[1] the social value of the facts published, [2] the depth of the article's intrusion into ostensibly private affairs, and [3] the extent to which the party voluntarily acceded to a position of public notoriety." ... Whether a publication is or is not newsworthy depends upon contemporary community mores and standards of decency. This is largely a question of fact, which a jury is uniquely well-suited to decide.

188 Cal. Rptr. 762, 779 (Cal. Ct. App. 1983) (citations omitted).

n50. As the court held in Michaels v. Internet Entm't Group, Inc.:

The first factor, the social value of the facts published, weighs against a finding of newsworthiness. It is difficult if not impossible to articulate a social value that will be advanced by dissemination of the Tape. The second factor, depth of intrusion, also weighs against a finding of newsworthiness. This factor is to be applied with an eye toward community mores as to the depth of intrusion... . At trial, it will be for the finder of fact to determine the state of community mores regarding the depth of intrusion... . For purposes of this motion, the Court determines that the plaintiffs are likely to convince the finder of fact that sexual relations are among the most private of private affairs, and that a video recording of two individuals engaged in such relations represents the deepest possible intrusion into such affairs. The third factor, voluntary accession to fame, weighs in favor of a finding of newsworthiness. Michaels and Lee declare that they have cultivated fame throughout their careers... . In Lee's case, her fame arises in part from television and movie roles based on sex and sexual appeal. The first two factors weigh heavily against a finding of newsworthiness for the contents of the Tape. The third factor weighs somewhat in favor of a finding of newsworthiness for the contents of the Tape. Weighing the factors together, the Court concludes that the plaintiffs have demonstrated a likelihood of success in meeting their burden to show that the contents of the Tape are not covered by the newsworthiness privilege.

5 F. Supp. 2d 823, 841-42 (C.D. Cal. 1998).

n51. In Miller v. California, 413 U.S. 15 (1973), the Supreme Court established a three-part test for obscenity, including an inquiry into whether the material taken as a whole, lacks serious literary, artistic, political, or scientific value:

The basic guidelines for the trier of fact must be: (a) whether "the average person, applying contemporary

community standards" would find that the work, taken as a whole, appeals to the prurient interest, ... (b) whether the work depicts or describes, in a patently offensive way, sexual conduct specifically defined by the applicable state law; and (c) whether the work, taken as a whole, lacks serious literary, artistic, political, or scientific value.

Id. at 24 (citations omitted). In obscenity cases, it is important to distinguish between that which is genuinely obscene and that which is merely indecent or offensive, such as material laced with vulgarity and sexually explicit language that does not appear to the prurient or erotic interest. For instance, as the court stated in United States v. Landham:

The Government failed to establish that Landham's phone calls were obscene communications. In his phone calls, Landham made comments such as, "herpes slut," "cuntless fuck," and "unmotherly piece of crap." These comments are admittedly "lewd, lascivious, filthy, or indecent." ... But they are not obscene. Landham's statements were invectives; he was swearing, vulgarly, at his wife because he was frustrated with their relationship. It could hardly be said that Landham's comments would appeal to the prurient interest of the average person.

251 F.3d 1072, 1086 (6th Cir. 2001).

n52. As the court held in Diaz v. Oakland Tribune, Inc.:

These same concerns are present in the related field of obscenity law, where community standards define what speech is constitutionally protected... . In an obscenity prosecution the jury is required to make an equally important constitutional decision and has been found to be up to the task... . Accordingly, where reasonable minds could differ, we see no constitutional infirmity in allowing the jury to decide the issue of newsworthiness.

188 Cal. Rptr. 762, 779 (Cal. Ct. App. 1983) (citing Miller v. California, 413 U.S. 15 (1973)); see Briscoe v. Reader's Digest Ass'n, 483 P.2d 34, 41 (Cal. 1971).

n53. Bartnicki v. Vopper, 532 U.S. 514, 518-19 (2001).

n54. The host of the show was named Frederick Vopper, though he appeared on the air under the name "Fred Williams."

n55. Bartnicki v. Vopper, 200 F.3d 109 (3d Cir. 1999).

n56. 408 U.S. 665 (1972).

n57. The opinion of the Court in Branzburg is literally permeated with rejection of the privilege, with scores of sentences expressing, in different ways, the Court's unwillingness to read such a privilege into the First Amendment. For instance, the Court stated as follows:

Of course, the press has the right to abide by its agreement not to publish all the information it has, but the right to withhold news is not equivalent to a First Amendment exemption from the ordinary duty of all other citizens to furnish relevant information to a grand jury performing an important public function.

Id. at 697. The Court continued:

We are admonished that refusal to provide a First Amendment reporter's privilege will undermine the freedom of the press to collect and disseminate news. But this is not the lesson history teaches us. As noted previously, the common law recognized no such privilege, and the constitutional argument was not even asserted until 1958. From the beginning of our country the press has operated without constitutional protection for press informants, and the press has flourished. The existing constitutional rules have not been a serious obstacle to either the development or retention of confidential news sources by the press.

Id. at 698. The Court elaborated:

It is said that currently press subpoenas have multiplied, that mutual distrust and tension between press and officialdom have increased, that reporting styles have changed, and that there is now more need for confidential sources, particularly where the press seeks news about minority cultural and political groups or dissident organizations suspicious of the law and public officials. These developments, even if true, are treacherous grounds for a far-reaching interpretation of the First Amendment fastening a nationwide rule on courts, grand juries, and prosecuting officials everywhere.

Id. at 699.

n58. Id. at 709 (Powell, J., concurring).

n59. In his concurrence, Justice Powell stated as follows:

The Court does not hold that newsmen, subpoenaed to testify before a grand jury, are without constitutional

rights with respect to the gathering of news or in safeguarding their sources. Certainly, we do not hold, as suggested in Mr. Justice Stewart's dissenting opinion, that state and federal authorities are free to "annex" the news media as "an investigative arm of government." ... If a newsman believes that the grand jury investigation is not being conducted in good faith he is not without remedy. Indeed, if the newsman is called upon to give information bearing only a remote and tenuous relationship to the subject of the investigation, or if he has some other reason to believe that his testimony implicates confidential source relationship without a legitimate need of law enforcement, he will have access to the court on a motion to quash and an appropriate protective order may be entered. The asserted claim to privilege should be judged on its facts by the striking of a proper balance between freedom of the press and the obligation of all citizens to give relevant testimony with respect to criminal conduct. The balance of these vital constitutional and societal interests on a case-by-case basis accords with the tried and traditional way of adjudicating such questions.

Id. at 709-10 (Powell, J., concurring).

n60. See, e.g., LaRouche v. Nat'l Broad. Co., 780 F.2d 1134 (4th Cir. 1986) (deciding that whether journalist's privilege will protect source depends upon whether the information sought is relevant, can be obtained by alternate means, and is the subject of a compelling interest); United States v. Burke, 700 F.2d 70 (2d Cir. 1983) (deciding that reporter's qualified privilege in criminal, as well as civil, cases is conditioned upon "clear and specific showing" that the information sought (1) is highly material and relevant, (2) is necessary or critical to the claim, and (3) is not obtainable from other available sources); Zerilli v. Smith, 656 F.2d 705 (D.C. Cir. 1981) (deciding that qualified privilege available under some circumstances in civil litigation, since Branzburg does not control in civil cases); United States v. Cuthbertson, 630 F.2d 139 (3d Cir. 1980) (finding that journalists have a federal common-law qualified privilege, in both civil and criminal cases, to refuse to divulge their sources); Miller v. Transamerican Press, Inc., 621 F.2d 721 (5th Cir. 1980) (reporter has First Amendment privilege which protects refusal to disclose identity of confidential informants, although privilege is not absolute).

n61. As the court held in In re Grand Jury Proceedings, Storer Communications, Inc. v. Giovan:

Accordingly, we decline to join some other circuit courts, to the extent that they have stated their contrary belief that those predicates do exist, and have thereupon adopted the qualified privilege balancing process urged by the three Branzburg dissenters and rejected by the majority... . That portion of Justice Powell's opinion certainly does not warrant the rewriting of the majority opinion to grant a first amendment testimonial privilege to news reporters, especially when the quoted language is considered in the context of that language which precedes it.

810 F.2d 580, 584 (6th Cir. 1987). Among courts that do recognize a reporter's privilege, there is a debate over whether it applies only to "confidential" material gathered by journalists, or to "nonconfidential" material as well, such as videotape "outtakes" from television interviews. Several circuits have extended the privilege to nonconfidential work product, either in civil or criminal cases. See, e.g., Shoen v. Shoen, 5 F.3d 1289, 1294-95 (9th Cir. 1993). Other courts, however, have refused to extend the privilege to nonconfidential material. See Gonzalez v. Nat'l Broad. Co., 155 F.3d 618 (2d Cir. 1998) (rejecting privilege as to nonconfidential material); United States v. Smith, 135 F.3d 963 (5th Cir. 1998) (refusing to apply privilege to nonconfidential videotape outtakes sought in a criminal proceeding); In re Shain, 978 F.2d 850, 853 (4th Cir. 1992) (rejecting tacitly the

privilege in a criminal case where the information sought was nonconfidential).

n62. Subsequent statements by the Supreme Court and individual Justices have advanced the ambiguity. In University of Pennsylvania v. EEOC, 493 U.S. 182, 201 (1990), for example, the Supreme Court stated: "In Branzburg, the Court rejected the notion that under the First Amendment a reporter could not be required to appear or to testify as to information obtained in confidence without a special showing that the reporter's testimony was necessary." And in New York Times, Co. v. Jascalevich, 439 U.S. 1301, 1302 (1978), Justice White writing an in-chambers single-Justice opinion denying a stay, stated: "There is no present authority in this Court that a newsman need not produce documents material to the prosecution or defense of a criminal case ... or that the obligation to obey an otherwise valid subpoena served on a newsman is conditioned upon the showing of special circumstances."

n63. Bartnicki v. Vopper, 532 U.S. 514, 535 (2001) (Breyer, J., concurring).

n64. See infra text accompanying notes 73-74.

n65. Bartnicki, 532 U.S. at 524-25.

n66. Id. at 525 (citing Florida Star v. B.J.F., 491 U.S. 524, 536 (1989) ("Even assuming the Constitution permitted a State to proscribe receipt of information, Florida has not taken this step.")).

n67. Id. at 548 (Rehnquist, C.J., dissenting); see infra text accompanying notes 224-241.

n68. Id. at 535 (Breyer, J., concurring); see infra text accompanying notes 198-223.

n69. Id. at 525.

If the statements about the labor negotiations had been made in a public arena - during a bargaining session, for example - they would have been newsworthy. This would also be true if a third party had inadvertently

overheard Bartnicki making the same statements to Kane when the two thought they were alone.

Id.

n70. Id. at 528.

n71. Id. (quoting Boehner v. McDermott, 191 F.3d 463, 484-85 (D.C. Cir. 1999) (Sentelle, J., dissenting)). The Court observed that its unwillingness to construe the question before it any more broadly was consistent with the "Court's repeated refusal to answer categorically whether truthful publication may ever be punished consistent with the First Amendment." Bartnicki, 532 U.S. at 529.

n72. See infra text accompanying notes 198-223.

n73. See infra text accompanying notes 79-87.

n74. See, e.g., Florida Star v. B.J.F., 491 U.S. 524 (1989) (applying "strict scrutiny" standard to privacy suit); Hazelwood v. Kuhlmeier, 484 U.S. 260 (1988) (establishing balancing test deferential to school officials for evaluating speech rights of students in public schools); Connick v. Myers, 461 U.S. 138 (1983) (establishing "issues of public concern" standard and balancing test for government employee speech claims); Cent. Hudson Gas & Elec. Corp. v. Pub. Serv. Comm'n, 447 U.S. 557 (1980) (creating four-part test for commercial speech); Miller v. California, 413 U.S. 15 (1973) (creating three-prong test for obscenity); Branzburg v. Hayes, 408 U.S. 665 (1972) (establishing balancing test for reporter's privilege); Red Lion Broad. Co. v. FCC, 395 U.S. 367 (1969) (establishing "intermediate scrutiny" standard for broadcast regulation); N.Y. Times Co. v. Sullivan, 376 U.S. 254 (1964) (establishing knowing or reckless disregard for truth or falsity standard for public official libels).

n75. See infra text accompanying notes 79-87.

n76. See infra text accompanying notes 91-95.

n77. See infra text accompanying notes 94-100.

n78. See infra text accompanying notes 112-114.

n79. Bartnicki v. Vopper, 532 U.S. 514, 536 (2001) (Breyer, J., concurring).

n80. The Chief Justice first declared flatly that the Court had applied strict scrutiny. Id. at 544 ("It nonetheless subjects these laws to the strict scrutiny normally reserved for governmental attempts to censor different viewpoints or ideas."). This was slightly qualified by another statement in which he accused the Court of "tacit" application of the standard. Id. ("There is scant support, either in precedent or in reason, for the Court's tacit application of strict scrutiny.").

n81. Id. at 531-32.

n82. See infra text accompanying notes 96-109.

n83. Bartnicki, 532 U.S. at 532 ("The justification for any such novel burden on expression must be "far stronger than mere speculation about serious harms.'") (quoting United States v. Nat'l Treasury Employees Union, 513 U.S. 454, 475 (1995)). In National Treasury Employees the Court struck down a ban on the receipt of honoraria by government employees for making speeches or writing articles. The Court in National Treasury Employees did not articulate a standard of review, but it clearly applied something less than strict scrutiny, conceding that the law was content-neutral and viewpoint-neutral, yet applying a standard more rigorous than the usual "Pickering-Connick" test applied in public employee speech cases. See Pickering v. Bd. of Educ., 391 U.S. 563 (1968); Connick v. Myers, 461 U.S. 138, 149 (1983); see also Waters v. Churchill, 511 U.S. 661 (1994).

n84. Bartnicki, 532 U.S. at 532 n.18 ("Indeed, even the burden of justifying restrictions on commercial speech requires more than "mere speculation or conjecture.'") (quoting Greater New Orleans Broad. Ass'n v. United States, 527 U.S. 173, 188 (1999)).

n85. Bartnicki, 532 U.S. at 532.

n86. Id. at 536 (Breyer, J., concurring).

n87. Id. at 544 (Rehnquist, C.J., dissenting).

n88. See Konigsberg v. State Bar, 366 U.S. 36, 50-51 (1961).

General regulatory statutes, not intended to control the content of speech but incidentally limiting its unfettered exercise, have not been regarded as the type of law the First or Fourteenth Amendment forbade Congress or the States to pass, when they have been found justified by subordinating valid governmental interests.

Id.

n89. See, e.g., Wisconsin v. Mitchell, 508 U.S. 476, 489-90 (1993) (upholding a hate-crime law that created enhanced penalties for bias-motivated crimes and refusing to apply heightened First Amendment scrutiny to the law, holding that the "First Amendment, moreover, does not prohibit the evidentiary use of speech to establish the elements of a crime or to prove motive or intent").

n90. See, e.g., Citizen Publ'g Co. v. United States, 394 U.S. 131 (1969) (sustaining application of antitrust laws to the press); Associated Press v. United States, 326 U.S. 1 (1945) (same); Okla. Press Publ'g Co. v. Walling, 327 U.S. 186 (1946) (sustaining application of Fair Labor Standards Act to the press); Associated Press v. NLRB, 301 U.S. 103 (1937) (sustaining application of National Labor Relations Act to the press).

n91. 501 U.S. 663 (1991).

n92. Id. at 669; see also Jimmy Swaggart Ministries v. Bd. of Equalization, 493 U.S. 378 (1990) (sustaining generally applicable tax laws as applied to religious institution); sources cited supra note 90.

n93. Cohen v. Cowles Media Co., 501 U.S. 663 (1991).

n94. See Reply Brief for the United States at 1-10, Bartnicki v. Vopper, 532 U.S. 514 (2001) (Nos. 99-1687 & 99-1728).

n95. See City of Erie v. Pap's A.M., 529 U.S. 277, 289 (2000) (plurality opinion) (stating that if the "governmental purpose in enacting the regulation is unrelated to the suppression of expression, then the regulation need only satisfy the "less stringent' standard from O'Brien"); Turner Broad. Sys., Inc. v. FCC, 512 U.S. 622, 641 (1994) (applying intermediate scrutiny because the law pursued "a legitimate regulatory goal" unrelated to the suppression of speech or the content of the message).

n96. Even those intermediate scrutiny opinions containing language that emphasizes the absence of viewpoint discrimination often go on to speak of the broader concept of content-based discrimination, appearing to acknowledge that content discrimination alone is enough to trigger strict scrutiny. See, e.g., City of Erie, 529 U.S. at 289 (plurality opinion) ("If the government interest is related to the content of the expression, ... then the regulation falls outside the scope of the O'Brien test.").

n97. See, e.g., Turner Broad. Sys., 512 U.S. at 643 (the government may not distinguish "favored speech from disfavored speech on the basis of the ideas or views expressed").

n98. See Columbia Broad. Sys., v. Democratic Nat'l Comm., 412 U.S. 94, 161 (1973) (Douglas, J., concurring) (describing ""rules that give one speaker, or viewpoint, less time (or none at all) to present a position,'" as ""a censorship ... as invidious as outright thought control.'" (quoting from the dissenting views of Federal Communications Commissioner Johnson)); Stanley v. Georgia, 394 U.S. 557, 566 (1969) ("Whatever the power of the state to control public dissemination of ideas inimical to the public morality, it cannot constitutionally premise legislation on the desirability of controlling a person's private thoughts.").

n99. See, e.g., United States v. Playboy Entm't Group, Inc., 529 U.S. 803 (2000); Reno v. ACLU, 521 U.S. 844 (1997); Sable Communications of Cal., Inc. v. FCC, 492 U.S. 115, 126 (1989).

n100. See Madsen v. Women's Health Ctr., Inc. 512 U.S. 753, 794 (1994) (Scalia, J., concurring in part and dissenting in part) ("The vice of content-based legislation - what renders it deserving of the high standard of strict scrutiny - is not that it is always used for invidious, thought-control purposes, but that it lends itself to use for those purposes."); City of Ladue v. Gilleo, 512 U.S. 43, 60 (1994) (O'Connor, J., concurring) (stating that strict scrutiny applies to content-based speech restrictions because such restrictions "are especially likely to be improper attempts to value some forms of speech over others, or are particularly susceptible to being used by the government to distort public debate").

n101. Ward v. Rock Against Racism, 491 U.S. 781, 791 (1988) (quoting Clark v. Cmty. for Creative Non-Violence, 468 U.S. 288, 293 (1984)).

n102. When legislatures classify on the basis of content the law will almost certainly be struck down when there is discontinuity between the governmental interests at stake and the classification the state has drawn. See, e.g., Simon & Schuster, Inc. v. Members of N.Y. State Crime Victims Bd., 502 U.S. 105, 120 (1991) (distinction drawn by Son of Sam law between income derived from criminal's descriptions of his crime and other sources "has nothing to do with" State's interest in transferring proceeds of crime from criminals to victims); Carey v. Brown, 447 U.S. 455, 465 (1980) (state's interest in residential privacy could not justify statute permitting labor picketing but prohibiting nonlabor picketing when "nothing in the content-based labor-nonlabor distinction has any bearing whatsoever on privacy"). One of the difficulties in classifying statutes that create privacy contraband is that there normally is not this same kind of blaring discontinuity; on the contrary, the statutes are normally targeted at precisely the privacy problem that the legislature sought to address. See supra text accompanying notes 7-27.

n103. See Providence Journal Co. v. FBI, 602 F.2d 1010, 1014 (1st Cir. 1979) ("The distinction between focusing on the content of information and on the manner of obtaining it blurs when the very manner of obtaining information carries such a likelihood of discovering private facts.").

n104. Bartnicki v. Vopper, 532 U.S. 514, 526 (2001) ("We agree with petitioners that 2511(1)(c), as well as its Pennsylvania analog, is in fact a content-neutral law of general applicability."). Justice Stevens made the point, however, that this classification is not always simple - an insight he would appear to immediately exploit in holding that the content-neutral law before the Court nevertheless had many attributes of a law that was content based. Id. ("Deciding whether a particular regulation is content based or content neutral is not always a simple task." (citing Turner Broad. Sys., Inc. v. FCC, 512 U.S. 622, 642 (1994))).

n105. Bartnicki, 532 U.S. at 526.

The statute does not distinguish based on the content of the intercepted conversations, nor is it justified by reference to the content of those conversations. Rather, the communications at issue are singled out by virtue of the fact that they were illegally intercepted - by virtue of the source, rather than the subject matter.

Id.

n106. Id.

n107. Id. at 528-29.

n108. Id. at 527 n.10. Justice Stevens took these examples from the brief of the United States filed by the Solicitor General to defend the statute. Id.; see also Fultz v. Gilliam, 942 F.2d 396, 400 n.4 (6th Cir. 1991) (statute applied in context of extortion); Dorris v. Absher, 959 F. Supp. 813, 815-17 (M.D. Tenn. 1997) (statute applied in context of workplace discipline), aff'd. in part, rev'd in part, 179 F.3d 420 (6th Cir. 1999); In re Grand Jury, 111 F.3d 1066, 1077-79 (3d Cir. 1997) (applying statute to bar even subsequent use in grand jury investigation).

n109. Bartnicki, 532 U.S. at 527.

It is true that the delivery of a tape recording might be regarded as conduct, but given that the purpose of such a delivery is to provide the recipient with the text of recorded statements, it is like the delivery of a handbill or a pamphlet, and as such, it is the kind of "speech" that the First Amendment protects.

Id. (citing Bartnicki v. Vopper, 200 F.3d 109, 120 (3d Cir 1999) ("If the acts of "disclosing' and "publishing' information do not constitute speech, it is hard to imagine what does fall within that category, as distinct from the category of expressive conduct.")).

n110. See supra text accompanying notes 87-93.

n111. See supra text accompanying notes 18-27.

n112. 391 U.S. 367 (1968).

n113. Id. at 377 (1968); see also Turner Broad. Sys. v. FCC, 512 U.S. 622, 662 (1994); Ward v. Rock Against Racism, 491 U.S. 781, 799 (1989).

n114. Ward, 491 U.S. at 799 (1989) (quoting United States v. Albertini, 472 U.S. 675, 689 (1985)).

n115. In constitutional law, variants of "intermediate scrutiny" are often employed to impose demanding standards of review considerably more rigorous than the highly deferential reasonableness or rational basis tests applied to mine-run economic and social legislation, yet not as demanding as such extremely high standards as "strict scrutiny," or "clear and present danger." The requirements that the government demonstrate "important" or "substantial" justifications for its actions and a "narrow tailoring" of ends to means are the touchstones of intermediate review. Intermediate scrutiny tests, varying slightly in their exact formulation as doctrinal contexts change, have thus been employed to impose significant protection against the abridgement of constitutional norms across the expanse of constitutional adjudication. See, e.g., United States v. Lopez, 514 U.S. 549, 558-59 (1995) (striking down federal legislation as exceeding Congress's power to regulate commerce, holding that to be upheld the law must regulate activity that has a "substantial relation" on interstate commerce); Miss. Univ. for Women v. Hogan, 458 U.S. 718, 724-25 (1982) (applying intermediate scrutiny in gender discrimination cases, requiring that state program be justified by a substantial governmental interest); Cent. Hudson Gas & Elec. Corp. v. Pub. Serv. Comm'n, 447 U.S. 557, 566 (1980) (adopting an intermediate level commercial speech standard requiring, among other things, that the regulation be supported by a "substantial" governmental interest and be "not more extensive than necessary" to serve that interest). When the Supreme Court requires a substantial nexus it appears to mean business, and has not tolerated slippage into the more deferential standards of rational basis review. See, e.g., 44 Liquormart v. Rhode Island, 517 U.S. 484 (1996) (applying intermediate commercial speech standard to strike down paternalistic regulation on liquor pricing, emphasizing need for rigorous review); United States v. Virginia, 515 U.S. 518, 533 (1996) (applying intermediate scrutiny in gender discrimination case, requiring that government justification be "exceedingly persuasive"). Indeed, when the Supreme Court has settled on a standard of review more rigorous than rational basis scrutiny, it has deliberately eschewed use of the terminology cast in the phrasings of "reasonable" relationships, precisely because of the danger that this standard will devolve into the pallid deference characteristic of rational basis review. In Dolan v. City of Tigard, the court stated:

We think the "reasonable relationship" test adopted by a majority of the state courts is closer to the federal constitutional norm than either of those previously discussed. But we do not adopt it as such, partly because the term "reasonable relationship" seems confusingly similar to the term "rational basis" which describes the minimal level of scrutiny under the Equal Protection Clause of the Fourteenth Amendment.

512 U.S. 374, 391 (1994).

n116. Bartnicki v. Vopper, 532 U.S. 514, 536-37 (2001) (Breyer, J., concurring); see infra text accompanying notes 196-197, 203-204.

n117. Bartnicki, 532 U.S. at 544 (Renhquist, C.J., dissenting); see infra text accompanying notes 226-227.

n118. See supra text accompanying notes 112-115.

n119. See, e.g., Butterworth v. Smith, 494 U.S. 624 (1990) (refusing to enforce the traditional veil of secrecy surrounding grand jury proceedings against a reporter who wished to disclose the substance of his own testimony after the grand jury had terminated, holding the restriction inconsistent with the First Amendment principle protecting disclosure of truthful information); Florida Star v. B.J.F., 491 U.S. 524 (1989) (holding unconstitutional the imposition of liability against a newspaper for publishing the name of a rape victim in contravention of a Florida statute prohibiting such publication in circumstances in which a police department inadvertently released the victim's name); Smith v. Daily Mail Publ'g Co., 443 U.S. 97, 104 (1979) (finding unconstitutional the indictment of two newspapers for violating a state statute forbidding newspapers to publish, without written approval of the juvenile court, the name of any youth charged as a juvenile offender, where the newspapers obtained the name of the alleged juvenile assailant from witnesses, the police, and a local prosecutor, stating that the "magnitude of the State's interest in this statute is not sufficient to justify application of a criminal penalty"); Landmark Communications, Inc. v. Virginia, 435 U.S. 829 (1978) (overturning criminal sanctions against newspaper for publishing information from confidential judicial disciplinary proceedings leaked to the paper); Cox Broad. Corp. v. Cohn, 420 U.S. 469 (1975) (holding unconstitutional a civil damages award entered against a television station for broadcasting the name of a rape-murder victim obtained from courthouse records).

n120. See Phila. Newspapers, Inc. v. Hepps, 475 U.S. 767, 778 (1986) (noting that "speech of public concern is at the core of the First Amendment's protections"); Garrison v. Louisiana, 379 U.S. 64, 74-75 (1964) (noting that when the law regulates discussion on "public affairs," truthful speech "may not be the subject of either civil or criminal sanctions," because such speech "is more than self-expression; it is the essence of self-government").

n121. The Daily Mail case, Smith v. Daily Mail Publ'g Co., 443 U.S. 97 (1979), has come to be seen as the case encapsulating the principle most succinctly. See id. at 103 ("If a newspaper lawfully obtains truthful information about a matter of public significance then state officials may not constitutionally punish publication of the information, absent a need to further a state interest of the highest order." (emphasis added)).

n122. The common-law right of publicity, for example, would not be possible if any truthful information that was deemed in some sense "newsworthy" could be published or broadcast in derogation of the right-holder. See, e.g., Zacchini v. Scripps-Howard Co., 433 U.S. 562, 575-79 (1977) (holding that First Amendment did not protect defendants from liability under the common-law tort of "appropriation" or "right of publicity" when news media filmed plaintiff's "human cannonball" act at a county fair and broadcast the act without the plaintiff's permission, holding that it was enough that defendants' knew that the plaintiff objected to the broadcast and went forward anyway); see also Harper & Row Publishers, Inc. v. Nation Enter., 471 U.S. 539, 568 (1985) (upholding copyright infringement action against The Nation magazine for printing excerpts from President Gerald Ford's memoirs, holding that the First Amendment did not shield the magazine from the normal principles of copyright liability); Snepp v. United States, 444 U.S. 507, 511-16 (1980) (upholding constructive

trust on defendants' book royalties for book published in violation of pre-clearance agreement with CIA); Goldstein v. California, 412 U.S. 546, 571 (1973) (upholding California's "record piracy" law, noting that "no restraint has been placed on the use of an idea or concept"). These issues, of course, shade into the problems discussed later in this Article, involving "intellectual property contraband" and "government secrets contraband." See infra text accompanying notes 278-295.

n123. For instance, in Florida Star v. B.J.F., the Court stated:

First, because the Daily Mail formulation only protects the publication of information which a newspaper has "lawfully obtained," ... the government retains ample means of safeguarding significant interests upon which publication may impinge, including protecting a rape victim's anonymity. To the extent sensitive information rests in private hands, the government may under some circumstances forbid its nonconsensual acquisition, thereby bringing outside of the Daily Mail principle the publication of any information so acquired.

491 U.S. 524, 534 (1989); see, e.g., Smith v. Daily Mail Pub'g Co., 443 U.S. 97, 103 (1979) ("None of these opinions directly controls this case; however, all suggest strongly that if a newspaper lawfully obtains truthful information about a matter of public significance then state officials may not constitutionally punish publication of the information, absent a need to further a state interest of the highest order." (emphasis added)); Landmark Communications, Inc. v. Virginia, 435 U.S. 829, 837 (1978) (noting that in the course of protecting a newspaper's First Amendment right to print confidential material from proceedings before Virginia's Judicial Inquiry and Review Commission, the Court's holding was not "concerned with the possible applicability of the statute to one who secures the information by illegal means and thereafter divulges it").

n124. As the Court stated in Florida Star:

The Daily Mail principle does not settle the issue whether, in cases where information has been acquired unlawfully by a newspaper or by a source, government may ever punish not only the unlawful acquisition, but the ensuing publication as well. This issue was raised but not definitively resolved in New York Times Co. v. United States and reserved in Landmark Communications. We have no occasion to address it here.

Florida Star, 491 U.S. at 535 n.8 (citations omitted) (citing N.Y. Times Co. v. United States, 403 U.S. 713 (1971); Landmark Communications, Inc. v. Virginia, 435 U.S. 829, 837 (1978)).

n125. 408 U.S. 665 (1972).

n126. Id. at 691.

n127. Id.

n128. 491 U.S. 524 (1989).

n129. Id. at 535 n.8 (emphasis added).

n130. Id. at 526 n.1 (prohibiting publication of "the name, address, or other identifying fact or information of the victim of any sexual offense"); Cox Broad. Corp. v. Cohen, 420 U.S. 469, 471 n.1 (1975) (prohibiting the publication of "the name or identity of any female who may have been raped or upon whom an assault with intent to commit rape may have been made").

n131. Smith v. Daily Mail Publ'g Co., 443 U.S. 97, 98 (1979) (barring publication of the name of any youth charged as a juvenile offender).

n132. Landmark Communications, Inc. v. Virginia, 435 U.S. 829, 831 (1978) (making it illegal to divulge the identification of any Judge who was the subject of an investigation and hearing before Virginia's Judicial Inquiry and Review Commission, the state commission charged with investigating ethics charges against judges).

n133. Butterworth v. Smith, 494 U.S. 624 (1990). In both Butterworth and Landmark the governmental restrictions were at least in part based on content, in the sense that they identified specific governmental proceedings and purported to restrict only speech arising from those proceedings. Yet in both cases the laws were also arguably content-neutral, in the sense that they were triggered without regard to what was said in the proceedings, and dealt more with where the speech had been taken from, not what it contained. Yet in both cases the interest the government sought to vindicate was largely based on the communicative impact of the expression. Landmark was particularly tainted in this respect; Virginia sought, among other things, to decrease the embarrassment felt by judges who were targets of an investigation, both to bolster public confidence in the judiciary and to make it easier to convince some judges under fire to quietly resign or retire. See Landmark, 435 U.S. at 833.

n134. Oklahoma Publ'g Co. v. Dist. Court, 430 U.S. 308 (1977) (per curiam) (involving a challenge to pretrial judicial order that enjoined members of the press from disclosing the name of a boy charged in a juvenile criminal proceeding).

n135. In Florida Star, for example, the law at issue was also not speaker neutral, but rather singled out the media for especially disfavored treatment. Florida Star simply did not answer the question of whether a speaker-neutral law that prohibited the dissemination of sensitive private information would always be unconstitutional. To the contrary, the case appeared to intimate that circumstances might exist in which the government could forbid the nonconsensual acquisition of private material, suggesting that a properly drawn law might be brought outside the Daily Mail principle that normally permits dissemination of truthful information lawfully obtained. See Florida Star v. B.J.F., 491 U.S. 524, 534 (1989) ("To the extent sensitive information rests in private hands, the government may under some circumstances forbid its nonconsensual acquisition, thereby bringing outside of the Daily Mail principle the publication of any information so acquired.").

n136. Olmstead v. United States, 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting).

n137. See generally Richard Posner, The Uncertain Protection of Privacy by the Supreme Court, 1979 Sup. Ct. Rev. 173.

n138. See, e.g., Hill v. Colorado, 530 U.S. 730, 716 (2000) ("The unwilling listener's interest in avoiding unwanted communication has been repeatedly identified in our cases. It is an aspect of the broader "right to be let alone.'"); Winston v. Lee, 470 U.S. 753, 758 (1985) (stating that the Fourth Amendment protects expectations of privacy, defined as "the individual's legitimate expectations that in certain places and at certain times he has "the right to be let alone'"); Stanley v. Georgia, 394 U.S. 557, 564 (1969) (quoting with approval Justice Brandeis's endorsement of the "right to be let alone" in Olmstead); Eisenstadt v. Baird, 405 U.S. 438, 453-54 n.10 (1972) (same).

n139. Hurley v. Irish-American Gay Group of Boston, 515 U.S. 557, 573 (1995) ("One important manifestation of the principle of free speech is that one who chooses to speak may also decide "what not to say.'" (quoting Pacific Gas & Elec. Co. v. Pub. Utilities Comm'n, 475 U.S. 1, 16 (1986)); Harper & Row, Publishers, Inc. v. Nation Enters., 471 U.S. 539, 559 (1985) ("There is necessarily, and within suitably defined areas, a concomitant freedom not to speak publicly, one which serves the same ultimate end as freedom of speech in its affirmative aspect." (quoting Estate of Ernest Hemingway v. Random House, 244 N.E.2d 250, 255 (N.Y. 1968))); Abood v. Detroit Bd. of Educ., 431 U.S. 209 (1977) (sustaining First Amendment right to withhold union dues spent on non-labor political issues with which the dues payer disagreed); Wooley v. Maynard, 430 U.S. 705 (1977) (holding that First Amendment gave Jehovah's Witness the right to cover up the New Hampshire state motto "Live Free or Die" on his license plate).

n140. See Boy Scouts of Am. v. Dale, 530 U.S. 640, 648 (2000) ("Forcing a group to accept certain members may impair the ability of the group to express those views, and only those views, that it intends to express."); Cal. Democratic Party v. Jones, 530 U.S. 567, 573-74 (2000) (stating that "a corollary of the right to associate is the right not to associate," describing this as the "First Amendment right to exclude"); Roberts v. United States Jaycees, 468 U.S. 609, 623 (1984) ("Freedom of association ... plainly presupposes a freedom not to associate.").

n141. See McIntyre v. Ohio Elections Comm'n, 514 U.S. 334 (1995) (protecting right to pass out anonymous political literature).

n142. In NAACP v. Alabama, 357 U.S. 449 (1958), the Supreme Court struck down Alabama's attempt to force the NAACP to disclose its membership list, observing that:

It is hardly a novel perception that compelled disclosure of affiliation with groups engaged in advocacy may constitute as effective a restraint on freedom of association as the forms of governmental action in the cases above were thought likely to produce upon the particular constitutional rights there involved. This Court has recognized the vital relationship between freedom to associate and privacy in one's associations.

Id. at 462. In Buckley v. Valeo, 424 U.S. 1 (1976), the Supreme Court upheld the disclosure provisions of the Federal Election Campaign Act. The Court in Buckley acknowledged that "compelled disclosure, in itself, can seriously infringe on privacy of association and belief guaranteed by the First Amendment" and that "significant encroachments on First Amendment rights of the sort that compelled disclosure imposes cannot be justified by a mere showing of some legitimate governmental interest" but must instead "survive exacting scrutiny." Id. at 64. The Court did leave open the possibility that in certain circumstances the disclosure provisions might violate the First Amendment, as applied to minor parties:

We are not unmindful that the damage done by disclosure to the associational interests of the minor parties and their members and to supporters of independents could be significant... . There could well be a case, similar to those before the Court in NAACP v. Alabama and Bates, where the threat to the exercise of First Amendment rights is so serious and the state interest furthered by disclosure so insubstantial that the Act's requirements cannot be constitutionally applied.

Id. at 71.

n143. See 2 Joseph Story, Commentaries on Equity Jurisprudence 220-21 (Arno Press 1972) (1836) (stating that publication of private correspondence "strikes at the root of all that free and mutual interchange of advice,

opinions, and sentiments, between relatives and friends, and correspondents, which is so essential to the wellbeing of society," because it compels "every one in self defence to write, even to his dearest friends, with the cold and formal severity, with which he would write to his wariest opponents, or most implacable enemies.").

n144. See Jaffee v. Redmond, 518 U.S. 1, 10 (1996) (noting that lack of confidentiality would impede effective psychotherapy); United States v. Nixon, 418 U.S. 683, 705 (1974) ("Human experience teaches that those who expect public dissemination of their remarks may well temper candor with a concern for appearances and for their own interests.").

n145. See United States v. Nixon, 418 U.S. 683, 708 (1974) ("The expectation of a President to the confidentiality of his conversations and correspondence ... has all the values to which we accord deference for the privacy of all citizens.").

n146. Swidler & Berlin v. United States, 524 U.S. 399, 407 (1998) (noting that fear of disclosure, even after death, could lead to withholding important information from legal counsel).

n147. See Nix v. O'Malley, 160 F.3d 343, 351 (6th Cir. 1998) ("The protection of privacy ... requires strict controls on the repetition of the contents of illegally intercepted communications" because "each time the illicitly obtained recording is replayed to a new and different listener, the scope of the invasion widens and the aggrieved party's injury is aggravated." (quoting Fultz v. Gilliam, 942 F.2d 396, 402 (6th Cir. 1991))).

n148. See Providence Journal Co. v. FBI, 602 F.2d 1010, 1013 (1st Cir. 1979) ("Congress' recognition of the victim's privacy as an end in itself recognizes that the invasion of privacy is not over when the interception occurs but is compounded by disclosure.").

n149. See Gelbard v. United States, 408 U.S. 41, 51-52 (1972) ("Contrary to the Government's assertion that the invasion of privacy is over and done with, to compel the testimony of these witnesses compounds the statutorily proscribed invasion of their privacy by adding to the injury of the interception the insult of compelled disclosure.").

n150. See supra note 5.

n151. See 2 Wayne R. LaFave & Austin W. Scott, Jr., Substantive Criminal Law 422, 810(a) (1986) (explaining that social policy rationale for making it a crime to receive stolen property is to remove the incentive to steal by drying up the market for stolen goods).

n152. 495 U.S. 103 (1990).

n153. 394 U.S. 557 (1969).

n154. Osborne involved an Ohio statute that, on its face, purported to prohibit the possession of "nude" photographs of minors. Osborne, 495 U.S. at 112. The Supreme Court recognized that "depictions of nudity, without more, constitute protected expression." Id. But as construed by the Ohio Supreme Court, the statute prohibited only "the possession or viewing of material or performance of a minor who is in a state of nudity, where such nudity constitutes a lewd exhibition or involves a graphic focus on the genitals, and where the person depicted is neither the child nor the ward of the person charged." Id. at 113. "By limiting the statute's operation in this manner," the Supreme Court held, "the Ohio Supreme Court avoided penalizing persons for viewing or possessing innocuous photographs of naked children." Id. at 113-14. The Supreme Court also found it significant that the Ohio Supreme Court concluded that the State must establish scienter in order to prove a violation of the law. Id. at 115.

n155. Id. at 109; see also New York v. Ferber, 458 U.S. 747, 760 (1982) ("The most expeditious if not the only practical method of law enforcement may be to dry up the market.").

n156. There is also an "exclusionary rule" applied under the Fifth Amendment for violations such as the failure to adhere to the principles applicable to the familiar Miranda warning. See Miranda v. Arizona, 384 U.S. 436, 479 (1966) (holding that certain warnings must be given before a suspect's statement made during custodial interrogation could be admitted in evidence); see also Dickerson v. United States, 530 U.S. 428 (2000) (""The Miranda exclusionary rule ... serves the Fifth Amendment and sweeps more broadly than that Amendment itself.'" (quoting Oregon v. Elstad, 470 U.S. 298, 306 (1985))). The phrase "exclusionary rule" is, however, most commonly associated with exclusions of evidence under the Fourth Amendment.

n157. See, e.g., Berry v. Funk, 146 F.3d 1003, 1011-13 (D.C. Cir. 1998) (deciding that Title III prohibited knowing investigatory use of unlawfully intercepted communications in a bona fide investigation of the inspector general); Chandler v. United States Army, 125 F.3d 1296, 1298-302 (9th Cir. 1997) (deciding that

United States Army is barred by Title III from exploiting illegally taped conversation to investigate charges of adultery); In re Grand Jury, 111 F.3d 1066, 1077-79 (3d Cir. 1997) (deciding that Title III prohibits disclosure of illegally recorded conversation to grand jury, despite the fact that the disclosure was in compliance with lawful subpoena).

n158. See Silverthorne Lumber Co. v. United States, 251 U.S. 385 (1920) (Holmes, J.). Although the Holmes opinion did not use the phrase "fruit of the poisonous tree," the phrase has since become the stock label for the doctrine. See, e.g., Costello v. United States, 365 U.S. 265, 278 (1961) ("It is argued that the wiretaps were illegal ... and that his admissions were therefore to be excluded from evidence as "fruit of the poisonous tree.'").

n159. As the Court stated in Silverthorne:

The proposition could not be presented more nakedly. It is that although of course its seizure was an outrage which the Government now regrets, it may study the papers before it returns them, copy them, and then may use the knowledge that it has gained to call upon the owners in a more regular form to produce them; that the protection of the Constitution covers the physical possession but not any advantages that the Government can gain over the object of its pursuit by doing the forbidden act... . In our opinion such is not the law. It reduces the Fourth Amendment to a form of words. The essence of a provision forbidding the acquisition of evidence in a certain way is that not merely evidence so acquired shall not be used before the Court but that it shall not be used at all. Of course this does not mean that the facts thus obtained become sacred and inaccessible. If knowledge of them is gained from an independent source they may be proved like any others, but the knowledge gained by the Government's own wrong cannot be used by it in the way proposed.

Silverthorne, 251 U.S. at 391-92.

n160. See Colorado v. Spring, 479 U.S. 564, 571-72 (1987) ("A confession cannot be "fruit of the poisonous tree' if the tree itself is not poisonous.").

n161. See, e.g., Pa. Bd. of Prob. & Parole v. Scott, 524 U.S. 357, 362-63 (1998) ("We have emphasized repeatedly that the governments' use of evidence obtained in violation of the Fourth Amendment does not itself violate the Constitution... . The exclusionary rule is instead a judicially created means of deterring illegal searches and seizures." (citing United States v. Leon, 468 U.S. 897, 906 (1984)); Stone v. Powell, 428 U.S. 465, 482, 486, 540 (1976); United States v. Calandra, 414 U.S. 338, 348 (1974).

n162. See, e.g., Scott, 524 U.S. at 369 (refusing to extend rule to parole revocation hearings); INS v.

Lopez-Mendoza, 468 U.S. 1032 (1984) (refusing to extend rule to civil deportation proceedings); United States v. Janis, 428 U.S. 433, 454 (1976) (holding that the exclusionary rule did not bar the introduction of unconstitutionally obtained evidence in a civil tax proceeding because the costs of excluding relevant and reliable evidence would outweigh the marginal deterrence benefits); United States v. Calandra, 414 U.S. 338, 351-52 (1974) (refusing to extend rule to grand jury proceedings).

n163. United States v. Calandra, 414 U.S. 338, 348 (1974); see also United States v. Janis, 428 U.S. 433, 454 (1976) ("If ... the exclusionary rule does not result in appreciable deterrence, then, clearly, its use in the instant situation is unwarranted").

n164. See, e.g., Scott, 524 U.S. at 364; United States v. Payner, 447 U.S. 727, 734 (1980) (arguing that the exclusionary rule's "costly toll" upon truth-seeking and law enforcement objectives presents a high obstacle for those urging application of the rule); Stone v. Powell, 428 U.S. 465, 490 (1976).

n165. For instance, as the Court stated in United States v. Leon:

Whether the exclusionary sanction is appropriately imposed in a particular case ... must be resolved by weighing the costs and benefits of preventing the use in the prosecution's case in chief of inherently trustworthy tangible evidence obtained in reliance on a search warrant issued by a detached and neutral magistrate that ultimately is found to be defective. The substantial social costs exacted by the exclusionary rule for the vindication of Fourth Amendment rights have long been a source of concern.

468 U.S. 897, 906-07 (1984).

n166. If the media were operating at arms length from the government, with no connection to it, incriminating evidence developed by the media and turned over to the government would presumably be excluded under the silver platter principle. If the media were acting in concert with the government, as in "ride-alongs," and in that context developed evidence through means that would normally violate the Fourth Amendment, one would expect the exclusionary rule to apply. The Supreme Court held, in the "ride-along" case, Wilson v. Lane, 526 U.S. 603 (1999), that the Fourth Amendment was violated by the presence of media during a police search. In a somewhat opaque footnote, the Court reserved judgment on whether the exclusionary rule would apply to evidence discovered or developed by media representatives. As the Court explained:

Even though such actions might violate the Fourth Amendment, if the police are lawfully present, the violation of the Fourth Amendment is the presence of the media and not the presence of the police in the home. We have no occasion here to decide whether the exclusionary rule would apply to any evidence discovered or developed by the media representatives.

Id. at 614 n.2.

n167. 256 U.S. 465 (1921).

n168. Id. at 470-71.

n169. Id. at 476.

n170. See, e.g., United States v. Jacobson, 466 U.S. 109, 113-14 (1984) ("This Court has also consistently construed this protection as proscribing only governmental action; it is wholly inapplicable "to a search or seizure, even an unreasonable one, effected by a private individual not acting as an agent of the Government or with the participation or knowledge of any governmental official.'" (quoting Walter v. United States, 447 U.S. 649, 662 (1980) (Blackmun, J., dissenting))); United States v. Janis, 428 U.S. 433, 455-56 n.31 (1976) ("It is well established, of course, that the exclusionary rule, as a deterrent sanction, is not applicable where a private party or a foreign government commits the offending act."). As the Court noted in Coolidge v. New Hampshire:

Had Mrs. Coolidge, wholly on her own initiative, sought out her husband's guns and clothing and then taken them to the police station to be used as evidence against him, there can be no doubt under existing law that the articles would later have been admissible in evidence... . The question presented here is whether the conduct of the police officers at the Coolidge house was such as to make her actions their actions for purposes of the Fourth and Fourteenth Amendments and their attendant exclusionary rules. The test, as the petitioner's argument suggests, is whether Mrs. Coolidge, in light of all the circumstances of the case, must be regarded as having acted as an "instrument" or agent of the state when she produced her husband's belongings.

403 U.S. 443, 487 (1971).

n171. Burdeau, 256 U.S. at 476-77 (Brandeis, J., dissenting). Justice Holmes joined Justice Brandeis's opinion.

n172. See Nixon v. Shrink Mo. Gov't PAC, 528 U.S. 377, 391 (2000) ("The quantum of empirical evidence needed to satisfy heightened judicial scrutiny of legislative judgments will vary up or down with the novelty and plausibility of the justification raised.").

n173. 408 U.S. 665 (1972).

n174. See supra text accompanying notes 56-61.

n175. As the Court noted in Branzburg:

The available data indicate that some newsmen rely a great deal on confidential sources and that some informants are particularly sensitive to the threat of exposure and may be silenced if it is held by this Court that, ordinarily, newsmen must testify pursuant to subpoenas, but the evidence fails to demonstrate that there would be a significant constriction of the flow of news to the public if this Court reaffirms the prior common-law and constitutional rule regarding the testimonial obligations of newsmen. Estimates of the inhibiting effect of such subpoenas on the willingness of informants to make disclosures to newsmen are widely divergent and to a great extent speculative. It would be difficult to canvass the views of the informants themselves; surveys of reporters on this topic are chiefly opinions of predicted informant behavior and must be viewed in the light of the professional self-interest of the interviewees. Reliance by the press on confidential informants does not mean that all such sources will in fact dry up because of the later possible appearance of the newsman before a grand jury.

Branzburg, 408 U.S. at 693-94. As previously noted, lower courts have split on whether to interpret Branzburg as creating a First Amendment reporter's privilege. See supra notes 60-61 and accompanying text.

n176. 395 U.S. 367 (1969).

n177. See generally Lee C. Bollinger, Images of a Free Press (1991); Lucas A. Powe, Jr., The Fourth Estate and the Constitution (1991); Cass R. Sunstein, Democracy and the Problem of Free Speech (1992); C. Edwin Baker, The Media That Citizens Need, 147 U. Pa. L. Rev. 317 (1998); Thomas G. Krattenmaker & L.A. Scott Powe, Jr., The Fairness Doctrine Today: A Constitutional Curiosity and an Impossible Dream, 1985 Duke L.J. 151; Steven Shiffrin, The Politics of the Mass Media and the Free Speech Principle, 69 Ind. L.J. 689 (1994).

n178. 376 U.S. 254 (1964).

n179. See David A. Anderson, Libel and Press Self-Censorship, 53 Tex. L. Rev. 422, 477 (1975).

n180. See generally Frederick Schauer, Fear, Risk and the First Amendment: Unraveling the "Chilling Effect," 58 B.U. L. Rev. 685, 696-97 (1978).

n181. For an historical overview and energetic defense of the Times case, and the many cases that it spawned, see Rodney A. Smolla, Suing the Press: Libel, the Media, and Power (1986). The definitive historical treatment of the case is Anthony Lewis, Make No Law: The Sullivan Case and the First Amendment (1991).

n182. The scholarly literature debating the Times decision is rich and formidable. See, e.g., Donald M. Gillmor, Power, Publicity, and the Abuse of Libel Law (1992); Lewis, supra note 181; Norman L. Rosenberg, Protecting the Best Men: An Interpretive History of the Law of Libel (1986); Robert Sack & Sandra Barron, Libel, Slander, and Related Problems (2d ed. 1996); Bruce W. Sanford, Libel and Privacy (2d ed. 1991); Rodney A. Smolla, supra note 181; Rodney A. Smolla, Law of Defamation (1999); Arthur L. Berney, Libel and the First Amendment - A New Constitutional Privilege, 51 Va. L. Rev. 1 (1965); William O. Bertelsman, The First Amendment and Protection of Reputation and Privacy - New York Times Co. v. Sullivan and How It Grew, 56 Ky. L.J. 718 (1967); William O. Bertelsman, Libel and Public Men, 52 A.B.A. J. 657 (1966); William J. Brennan, Jr., The Supreme Court and the Meiklejohn Interpretation of the First Amendment, 79 Harv. L. Rev. 1 (1965); T. Barton Carter, Right of Reply Versus the Sullivan Rule: Time for a Second Look, 27 Loy. L. Rev. 41 (1981); Lewis C. Green, The New York Times Rule: Judicial Overkill, 12 Vill. L. Rev. 730 (1967); Harry Kalven, The New York Times Case: A Note on "The Central Meaning of the First Amendment," 1964 Sup. Ct. Rev. 191; Anthony Lewis, New York Times v. Sullivan Reconsidered: Time to Return to "The Central Meaning of the First Amendment," 83 Colum. L. Rev. 603 (1983); Jerome L. Merin, Libel and the Supreme Court, 11 Wm. & Mary L. Rev. 371 (1969); Harold L. Nelson, Newsmen and the Times Doctrine, 12 Vill. L. Rev. 738 (1967); Bruce L. Ottley et al., New York Times v. Sullivan: A Retrospective Examination, 33 DePaul L. Rev. 741 (1984); Willard H. Pedrick, Freedom of the Press and the Law of Libel: The Modern Revised Translation, 49 Cornell L.Q. 581 (1964); Samuel R. Pierce, The Anatomy of a Historic Decision, New York Times Co. v. Sullivan, 43 N.C. L. Rev. 315 (1965); Rodney A. Smolla, Let the Author Beware: The Rejuvenation of the American Law of Libel, 132 U. Pa. L. Rev. 1 (1983).

n183. See supra text accompanying notes 17-27.

n184. Bartnicki v. Vopper, 532 U.S. 514, 529 (2001) ("The normal method of deterring unlawful conduct is to impose an appropriate punishment on the person who engages in it.").

n185. Id.

n186. Id.

n187. Id. at 530 n.13 (citing Osborne v. Ohio, 495 U.S. 103 (1990)); New York v. Ferber, 458 U.S. 747, 762 (1982) ("The value of permitting live performances and photographic reproductions of children engaged in lewd sexual conduct is exceedingly modest, if not de minimis.").

n188. Bartnicki, 532 U.S. at 530 n.13.

n189. Id. at 530.

n190. Id. at 518.

n191. Id. at 532 (citing Harper & Row, Publishers, Inc. v. Nation Enter., 471 U.S. 539, 559 (1985)). The Court also accepted that there were important interests on both sides of the constitutional equation:

Accordingly, it seems to us that there are important interests to be considered on both sides of the constitutional calculus. In considering that balance, we acknowledge that some intrusions on privacy are more offensive than others, and that the disclosure of the contents of a private conversation can be an even greater intrusion on privacy than the interception itself.

Bartnicki, 532 U.S. at 533.

n192. The Court noted:

If the statements about the labor negotiations had been made in a public arena - during a bargaining session, for example - they would have been newsworthy. This would also be true if a third party had inadvertently overheard Bartnicki making the same statements to Kane when the two thought they were alone.

Id. at 525.

n193. See infra text accompanying notes 196-218.

n194. Bartnicki, 532 U.S. at 535 (Breyer, J., concurring).

n195. Id. at 535-36 (emphasis added).

n196. Id. at 536 (quoting Olmstead v. United States, 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting)).

n197. Id. at 536 (Breyer, J., concurring).

n198. Id. at 537.

n199. Id. (emphasis added).

n200. Id.

n201. Id. (citing Gelbard v. United States, 408 U.S. 41, 51-52 (1972)).

n202. Id. at 537 (Breyer, J., concurring).

n203. Id. (citing Warren & Brandeis, The Right to Privacy, 4 Harv. L. Rev. 193 (1890); Restatement (Second) of Torts 652D (1977); Katz v. United States, 389 U.S. 347, 350-51 (1967) ("The protection of a person's general right to privacy - his right to be let alone by other people - is, like the protection of his property and of his very life, left largely to the law of the individual States.")).

n204. Bartnicki, 532 U.S. at 538 (Breyer, J., concurring).

n205. Id.

n206. Id.

n207. Id. (citing 18 U.S.C. 2, "criminalizing aiding and abetting any federal offense," and 2 W. LaFave & A. Scott, Substantive Criminal Law 6.6(b)-(c) (1986), "describing criminal liability for aiding and abetting").

n208. Bartnicki, 532 U.S. at 538 (Breyer, J., concurring).

n209. Id. ("The Court adds that its holding "does not apply to punishing parties for obtaining the relevant information unlawfully.'" (quoting id. at 532 n.19 (opinion of the Court))).

n210. Id. at 539 (Breyer, J., concurring) (second emphasis added).

n211. Id. (citing Restatement (Second) of Torts 595 cmt. g (1977), stating "general privilege to report that "another intends to kill or rob or commit some other serious crime against a third person'"; Restatement (Second) of Torts 652G, stating that "privilege applies to invasion of privacy tort"; Restatement (Third) of Unfair Competition 40 cmt. c (1995), stating that "trade secret law permits disclosures relevant to public health or safety, commission of crime or tort, or other matters of substantial public concern"; Lachman v. Sperry-Sun Well Surveying Co., 457 F.2d 850, 853 (10th Cir. 1972), finding "nondisclosure agreement not binding with respect to criminal activity"; Tarasoff v. Regents of Univ. of Cal., 551 P.2d 334, 343-44 (Cal. Ct. App. 1976), finding "psychiatric privilege not binding in presence of danger to self or others").

n212. Bartnicki, 532 U.S. at 539-40 (Breyer, J., concurring) (citing Wolston v. Reader's Digest Ass'n, 443 U.S. 157, 164 (1979); Hutchinson v. Proxmire, 443 U.S. 111, 134 (1979); Gertz v. Robert Welch, Inc., 418 U.S. 323, 351 (1974); Warren & Brandeis, supra note 203, at 215). The citations to the Wolston, Hutchinson, and Gertz cases are not particularly forceful in this context. In all three cases, the Supreme Court held that the plaintiffs, each of whom had certainly obtained some degree of prominence and notoriety, were in fact properly classified as private figures.

n213. Bartnicki, 532 U.S. at 534.

n214. Id. at 540 (Breyer, J., concurring).

n215. Id. ("But the subject matter of the conversation at issue here is far removed from that in situations where the media publicizes truly private matters." (citing Michaels v. Internet Entm't Group, Inc., 5 F. Supp. 2d 823, 841-42 (C.D. Cal. 1998), finding "broadcast of videotape recording of sexual relations between famous actress and rock star not a matter of legitimate public concern"; W. Page Keeton et al., Prosser & Keeton on the Law of Torts 117 (W. Page Keeton ed., 5th ed. 1984), "stating that there is little expectation of privacy in mundane facts about a person's life, but that "portrayal of ... intimate private characteristics or conduct' is "quite a different matter'"; Warren & Brandeis, supra note 203, at 214, "recognizing that in certain matters "the community has no legitimate concern'"; Time, Inc. v. Firestone, 424 U.S. 448, 454-55 (1976), finding that "despite interest of public, divorce of wealthy person not a "public controversy'")).

n216. Bartnicki, 532 U.S. at 540 (Breyer, J., concurring).

n217. Id.

n218. Id. (emphasis added).

n219. See supra text accompanying notes 208-209.

n220. Bartnicki, 532 U.S. at 541 (Breyer, J., concurring).

n221. Id.

n222. Id. ("Eavesdropping on ordinary cellular phone conversations in the street (which many callers seem to tolerate) is a very different matter from eavesdropping on encrypted cellular phone conversations or those carried on in the bedroom.").

n223. In his concurrence, Justice Breyer noted:

But the technologies that allow the former may come to permit the latter. And statutes that may seem less important in the former context may turn out to have greater importance in the latter. Legislatures also may decide to revisit statutes such as those before us, creating better tailored provisions designed to encourage, for example, more effective privacy-protecting technologies.

For these reasons, we should avoid adopting overly broad or rigid constitutional rules, which would unnecessarily restrict legislative flexibility. I consequently agree with the Court's holding that the statutes as applied here violate the Constitution, but I would not extend that holding beyond these present circumstances.

Id.

n224. Id. (Rehnquist, C.J., dissenting).

n225. Id.

n226. Id.

n227. Id. at 548.

n228. Id. at 545.

n229. Id. at 546.

n230. Id.

n231. Id.

n232. Id.

n233. Id. at 547 ("But fear of "timidity and self-censorship' is a basis for upholding, not striking down, these antidisclosure provisions: They allow private conversations to transpire without inhibition.").

n234. Id.

n235. Id. at 547 n.4. The federal statute, for example, was specifically amended in 1986, when Congress increased the scienter requirement from "willful" to "intentional." See 18 U.S.C. 2511(1)(c); see also S. Rep. No. 99-541, at 6 (1986) ("In order to underscore that the inadvertent reception of a protected communication is not a crime, the subcommittee changed the state of mind requirement under title III ... from "willful' to "intentional.'").

n236. Bartnicki, 532 U.S. at 548 (Rehnquist, C.J., dissenting).

n237. Id. (emphasis added).

n238. Id.

n239. Id. at 550 (citing 2 W. LaFave & A. Scott, Substantive Criminal Law 8.10(a) (1986) ("Without such receivers, theft ceases to be profitable. It is obvious that the receiver must be a principal target of any society anxious to stamp out theft in its various forms")).

n240. Bartnicki, 532 U.S. at 551 (Rehnquist, C.J., dissenting).

n241. Id. at 554 (estimating that "49.1 million analog cellular telephones are currently in operation") (citing Hao, Nokia Profits from Surge in Cell Phones, Fla. Today, July 18, 1999, at E1).

n242. See Eugene Volokh, Freedom of Speech and Information Privacy: The Troubling Implications of a Right to Stop People from Speaking About You, 52 Stan. L. Rev. 1049, 1107-10 (2000).

n243. Id; see also R.A.V. v. City of St. Paul, 505 U.S. 377 (1992) (striking down hate-speech law); Smolla, Free Speech, supra note 38, at 151-69 (arguing in favor of tolerating intolerance).

n244. The substantive analysis on this has already been made, and will not be repeated here. See supra text accompanying notes 192-241.

n245. See supra text accompanying notes 214, 233.

n246. In the specific context of Title III, for example, it appears most sensible to treat the law as content-neutral, insofar as it merely deals with how material was gathered. See, e.g., Boehner v. McDermott, 191 F.3d 463, 467 (D.C. Cir. 1999). And this was, indeed, how a majority of the Justices (and arguably all nine) saw the case.

n247. See supra text accompanying notes 79-87.

n248. Many of the "truthful publication" cases that have reached the Supreme Court have been content based in this sense, limiting their application to defined subject matter. See Florida Star v. B.J.F., 491 U.S. 524, 526 n.1 (1989) (prohibiting publication of "the name, address, or other identifying fact or information of the victim of any sexual offense"); Smith v. Daily Mail Publ'g Co., 443 U.S. 97, 98 (1979); (barring publication of the name of any youth charged as a juvenile offender); Landmark Communications, Inc. v. Virginia, 435 U.S. 829, 831 (1978) (making it illegal to divulge the identification of any judge who was the subject of an investigation and hearing before the Virginia Judicial Inquiry and Review Commission, the state commission charged with investigating ethics charges against judges); Okla. Publ'g Co. v. Dist. Ct., 430 U.S. 308 (1977) (per curiam) (considering a challenge to pretrial judicial order that enjoined members of the press from disclosing the name of a boy charged in a juvenile criminal proceeding); Cox Broad. Corp. v. Cohn, 420 U.S. 469, 471 n.1 (1975) (prohibiting the publication of "the name or identity of any female who may have been raped or upon whom an assault with intent to commit rape may have been made").

n249. See Bartnicki v. Vopper, 532 U.S. 514, 555 (2001) (Rehnquist, C.J., dissenting) ("Although public persons may have forgone the right to live their lives screened from public scrutiny in some areas, it does not and should not follow that they also have abandoned their right to have a private conversation without fear of it being intentionally intercepted and knowingly disclosed.").

n250. Id.

n251. Id. at 525 & n.8 (citing New York Times Co. v. Sullivan, 376 U.S. 254, 265-66 (1964); First Nat'l Bank of Boston v. Bellotti, 435 U.S. 765, 777 (1978)).

n252. See supra notes 56-61 and accompanying text.

n253. In Richmond Newspapers, Inc. v. Virginia, 448 U.S. 555 (1980), the Supreme Court recognized a First Amendment right of access to criminal trials, and numerous subsequent decisions of the Court reinforced and elaborated upon that right. See, e.g., Globe Newspaper Co. v. Superior Ct., 457 U.S. 596 (1982); Press-Enter. Co. v. Superior Ct., 464 U.S. 501 (1984); Waller v. Georgia, 467 U.S. 39 (1984); Press-Enter. Co. v. Super. Ct., 478 U.S. 1 (1986) (Press-Enterprise II); El Vocero de Puerto Rico v. Puerto Rico, 508 U.S. 147 (1993). The Court has refused to create any broader First Amendment access rights, however. See, e.g., Pell v. Procunier, 417 U.S. 817 (1974) (refusing to recognize the press's right of access to prisons and jails over and above the rights those institutions afford to members of the general public); Saxbe v. Wash. Post Co., 417 U.S. 843 (1974) (same); Houchins v. KQED, Inc., 438 U.S. 1 (1978) (same).

n254. See generally Rodney A. Smolla, Smolla and Nimmer on Freedom of Speech 22:1-22:24 (3d ed. 2000) (discussing the "Uncertain Significance of the Press Clause"). The Court has routinely struck down laws that singled out the institutional press for disfavored treatment. See, e.g., Florida Star v. B.J.F., 491 U.S. 524, 540-41 (1989); Ark. Writers' Project, Inc. v. Ragland, 481 U.S. 221, 229 (1987); Minneapolis Star & Tribune Co. v. Minn. Comm'r of Revenue, 460 U.S. 575, 585 (1983); Smith v. Daily Mail Publ'g Co., 443 U.S. 97, 101-02 (1979); Miami Herald Publ'g Co. v. Tornillo, 418 U.S. 241 (1974).

n255. See supra notes 56-61.

n256. See George W. Conk, Is There a Design Defect in the Restatement (Third) of Torts: Products Liability?, 109 Yale L.J. 1087 (2000).

n257. Id. at 1092-98.

n258. Id. at 1094 ("Blood products, too, were branded as "unavoidably unsafe.' This determination was codified by forty-seven states in "blood shield laws' that protected sellers of blood and blood products from strict-liability and warranty claims. Negligence claims for blood products usually were permitted, but were practically impossible for plaintiffs to win.").

n259. This is analogous to the "social compact" of sorts embedded in products liability law and its regime of manufacturer liability for defective products. See Restatement (Second) of Torts 402A (1965). "Comment K" of the Restatement (Second) contained the exemption for products that were "unavoidably unsafe."

n260. The lack of such a scientific test ought to arguably be the touchstone for the true unavoidably unsafe product. The assumption that this is the case was made for blood, for example, though it turned out, in hindsight, to not be scientifically accurate. See Conk, supra note 256, at 1094.

n261. See supra text accompanying notes 44-48. There may be an analogy here as well to the "consumer expectations" test for strict products liability, which held prominence in 402A of the Restatement (Second) of Torts and remains the test in many jurisdictions today despite the Restatement (Third)'s move toward the negligence standard of "reasonable alternative design." The consumer expectation test, like the question of what constitutes "public" and "private" matters, can be viewed in one sense as a matter of social convention.

n262. See supra text accompanying notes 120-121.

n263. See supra text accompanying notes 120-123.

n264. See 17 U.S.C. 102 (1990) (defining general subject matter of copyright).

n265. See Harper & Row, Publishers, Inc. v. Nation Enters., 471 U.S. 539, 556 (1985) ("Copyright's idea/expression dichotomy "strikes a definitional balance between the First Amendment and the Copyright Act by permitting free communication of facts while still protecting an author's expression.'" (citing Harper & Row, Publishers, Inc. v. Nation Enters., 723 F.2d 195, 203 (2d Cir. 1983)).

n266. The United States Court of Appeals for the District of Columbia Circuit in Eldred v. Reno, 239 F.3d 372 (D.C. Cir. 2001), cert. granted, Eldred v. Ashcroft, 122 S. Ct. 1062 (Feb. 19, 2002) (No. 01-618), upheld the Copyright Term Extension Act of 1998 ("CTEA"), Pub. L. No. 105-298, 112 Stat. 2827 (1998). The case presented a constitutional challenge under the First Amendment and the Copyright Clause to the power of Congress to extend for a period of years the duration of copyrights, both those already extant and those yet to come. The court rejected both constitutional claims, pointedly cutting off at the threshold any First Amendment challenge to the copyright extension:

The decisions of the Supreme Court ... and of this court ... stand as insuperable bars to plaintiffs' first amendment theory... . [In Harper & Row] the Court explained how the regime of copyright itself respects and adequately safeguards the freedom of speech protected by the First Amendment.

... .

In keeping with this approach, we held ... that copyrights are categorically immune from challenges under the First Amendment... .

... .

... We think the plaintiffs' purported distinction is wholly illusory. The relevant question under the First Amendment - regardless whether it arises as a defense in a suit for copyright infringement or in an anticipatory challenge to a statute or regulation - is whether the party has a first amendment interest in a copyrighted work. The works to which the CTEA applies, and in which plaintiffs claim a first amendment interest, are by definition under copyright; that puts the works on the latter half of the "idea/expression dichotomy" and makes them subject to fair use. This obviates further inquiry under the First Amendment... .

... Suffice it to say we reject their first amendment objection to the CTEA because the plaintiffs lack any cognizable first amendment right to exploit the copyrighted works of others.

Eldred, 239 F.3d at 375-76 (citations omitted).

n267. See, e.g., Gertz v. Robert Welch, Inc., 418 U.S. 323 (1974) (adopting First Amendment distinction between public and private figure defamation standards and establishing various limitations on damages); N.Y. Times Co. v. Sullivan, 376 U.S. 254 (1964) (first imposing First Amendment "actual malice" standard in public official defamation cases).

n268. See Phila. Newspapers, Inc. v. Hepps, 475 U.S. 767 (1986) (finding that burden is on plaintiff to prove falsity in defamation actions, at least when there is a media defendant and speech is on matters of public concern).

n269. See Milkovich v. Lorain Journal Co., 497 U.S. 1 (1990).

n270. See Liberty Lobby, Inc. v. Dow Jones & Co., 838 F.2d 1287, 1298 (D.C. Cir.) ("The common law of libel has long held that one who republishes a defamatory statement "adopts' it as his own, and is liable in equal measure to the original defamer.") (citing Dameron v. Wash. Magazine, Inc., 779 F.2d 736, 739 (D.C. Cir. 1985); W. Page Keeton et al., Prosser & Keeton on the Law of Torts 117 (W. Page Keeton ed., 5th ed. 1984).

n271. See, e.g., Baskin v. Rogers, 493 S.E.2d 728, 730 (Ga. Ct. App. 1997).

Claiming she only told others that she had heard of the affairs, not that the affairs were fact, Rogers contends this does not constitute slander. But "talebearers are as bad as talemakers." Every repetition of a slander originated by a third person is a willful [sic] publication of it, rendering the person so repeating it liable to an action, and it is no defense that the speaker did not originate the slander, but heard it from another, even though he in good faith believed it to be true.

Id.; McDonald v. Glitsch, Inc., 589 S.W.2d 554, 556 (Tex. Civ. App. 1979) ("Every repetition of a slander is a willful publication of it, rendering the speaker liable to an action. Talebearers are as bad as talemakers." (quoting Houston Chronicle Publ'g Co. v. Wegner, 182 S.W. 45 (Tex. Civ. App. 1915)).

n272. See McCracken v. Gainesville Tribune Co., 246 S.E.2d 360, 362 (Ga. Ct. App. 1978) (deciding that newspaper may be held liable for defamation "even though the source of the communication is quoted, for the law holds that "talebearers are as bad as talemakers'" (citations omitted)). As William Prosser long ago explained, "Every repetition of the defamation is a publication in itself, even though the repeater states the source, or resorts to the customary newspaper evasion "it is alleged' ... ." William Prosser, Law of Torts, 113 (4th ed. 1971); see also W. Page Keeton et al., Prosser & Keeton on the Law of Torts 117 (W. Page Keeton ed., 5th ed. 1984).

n273. See Edwards v. Nat'l Audubon Soc'y, 556 F.2d 113 (2d Cir. 1977).

n274. For instance, in Sherwood v. Evening News Ass'n, the court stated:

It is well settled that a faithful and fair report of the proceedings in courts of justice are privileged, even though the reputation [sic] of individuals incidentally suffer from their publication, and for the publication of faithful, true, and fair reports of judicial proceedings publishers are neither civilly nor criminally liable.

239 N.W. 305, 306 (Mich. 1931) (citing Wason v. Walter, 4 L.R.-Q.B. 73 (1868); Bromage v. Prosser, 107 Eng. Rep. 1051 (K.B. 1825), Taylor v. Hawkins, 117 Eng. Rep. 897 (Q.B. 1851); Davison v. Duncan, 119 Eng. Rep. 1233 (Q.B. 1857)).

n275. Cowley v. Pulsifer, 137 Mass. 392, 394 (1884) (citing Rex v. Wright, 101 Eng. Rep. 1396 (K.B. 1799)).

n276. For example, in In re Charlotte Observer, 921 F.2d 47 (4th Cir. 1990) (per curiam), the court struck

down an order prohibiting reporters from revealing the fact, disclosed inadvertently in open court when two reporters were present, that an attorney was under grand jury investigation, noting:

On the present record, however, "the cat is out of the bag." The district court did not close the hearing and the disclosure was made in the courtroom, a particularly public forum. Once announced to the world, the information lost its secret characteristic, an aspect that could not be restored by the issuance of an injunction to two reporters.

Id. at 50.

n277. See 17 U.S.C. 105 (1976) (denying copyright protection to works of the United States Government); see also Schnapper v. Foley, 667 F.2d 102 (D.C. Cir. 1981) (interpreting 105).

n278. See Harper & Row, Publishers, Inc. v. Nation Enters., 471 U.S. 539, 560 (1985) ("In view of the First Amendment protections already embodied in the Copyright Act's distinction between copyrightable expression and uncopyrightable facts and ideas, and the latitude for scholarship and comment traditionally afforded by fair use, we see no warrant for expanding the doctrine of fair use ... ."). Similarly, in the Supreme Court's other modern "fair use" decisions, Sony Corp. of America v. Universal City Studios, Inc., 464 U.S. 417 (1984), and Campbell v. Acuff-Rose Music, Inc., 510 U.S. 569 (1994), the First Amendment "strict scrutiny" test is never mentioned, and the decisions focus on the self-contained contours of copyright doctrine.

n279. See, e.g., Harper & Row, 471 U.S. at 558 ("In our haste to disseminate news, it should not be forgotten that the Framers intended copyright itself to be the engine of free expression. By establishing a marketable right to the use of one's expression, copyright supplies the economic incentive to create and disseminate ideas." (citing Mazer v. Stein, 347 U.S. 201, 219 (1954) ("The economic philosophy behind the clause empowering Congress to grant patents and copyrights is the conviction that encouragement of individual effort by personal gain is the best way to advance public welfare through the talents of authors and inventors in "Science and useful Arts.'")); Twentieth Century Music Corp. v. Aiken, 422 U.S. 151, 156 (1975) ("The immediate effect of our copyright law is to secure a fair return for an "author's' creative labor. But the ultimate aim is, by this incentive, to stimulate [the creation of useful works] for the general public good.").

n280. See Iowa State Univ. Research Found., Inc. v. Am. Broad. Cos., 621 F.2d 57, 61 (2d Cir. 1980) ("The fair use doctrine is not a license for corporate theft, empowering a court to ignore a copyright whenever it determines the underlying work contains material of possible public importance.").

n281. Article I grants to Congress the power "to promote the Progress of Science and useful Arts, by

securing for limited Times to Authors and Inventors the exclusive Right to their respective Writings and Discoveries." U.S. Const. art. I, 8, cl. 8. In Goldstein v. California, 412 U.S. 546, 561 (1973), the Supreme Court acknowledged the commodious sweep of this constitutional grant, observing that the terms of the Copyright Clause "have not been construed in their narrow literal sense but, rather, with the reach necessary to reflect the broad scope of constitutional principles." The Necessary and Proper Clause in turn empowers Congress to "make all Laws which shall be necessary and proper for carrying into Execution the foregoing Powers." U.S. Const. art. I, 8, cl. 18. For two centuries the Necessary and Proper Clause has been read as a munificent expansion of Congress' power under Article I, not as a narrow confinement of it. As Chief Justice John Marshall admonished:

It must have been the intention of those who gave these powers, to insure, as far as human prudence could insure, their beneficial execution. This could not be done by confiding the choice of means to such narrow limits as not to leave it in the power of Congress to adopt any which might be appropriate, and which were conducive to the end.

McCulloch v. Maryland, 17 U.S. (4 Wheat.) 316, 415 (1819).

n282. See, e.g., N.Y. Times Co. v. United States, 403 U.S. 713, 726 n. (1971) (Brennan, J., concurring). Justice Brennan distinguished the prior restraint at issue in the famous "Pentagon Papers" case from protection of copyright, stating:

Similarly, copyright cases have no pertinence here: the Government is not asserting an interest in the particular form of words chosen in the documents, but is seeking to suppress the ideas expressed therein. And the copyright laws, of course, protect only the form of expression and not the ideas expressed.

Id.; see also id. at 731-32 n.1 (1971) (White, J., concurring) ("No one denies that a newspaper can properly be enjoined from publishing the copyrighted works of another."); New Era Publ'ns, Int'l, APS v. Henry Holt & Co., 695 F. Supp. 1493, 1525 (S.D.N.Y. 1988) ("Injunctions are generally issued to prevent infringement of copyright."), aff'd, 873 F.2d 576, 584 (2d Cir. 1989).

n283. See, e.g., Nihon Keizai Shimbun v. Comline Bus. Data, Inc., 166 F.3d 65, 74 (2d Cir. 1999) ("Defendants argue that this injunction is overly broad and represents an unconstitutional prior restraint on freedom of the press... . We have repeatedly rejected First Amendment challenges to injunctions from copyright infringement on the ground that First Amendment concerns are protected by and coextensive with the fair use doctrine."). In Dallas Cowboys Cheerleaders, Inc. v. Pussycat Cinema, Ltd., the court noted:

For similar reasons, the preliminary injunction did not constitute an unconstitutional "prior restraint." This is not a case of government censorship, but a private plaintiff's attempt to protect its property rights. The propriety of a preliminary injunction where such relief is sought is so clear that courts have often issued an injunction without even mentioning the first amendment... . The prohibition of the Lanham Act is content neutral, ... and therefore

does not arouse the fears that trigger the application of constitutional "prior restraint" principles.

604 F.2d 200, 206 (2d Cir. 1979) (citations omitted); see also Abkco Music, Inc. v. Stellar Records, Inc., 96 F.3d 60 (2d Cir. 1996) ("Generally when a copyright plaintiff makes out a prima facie showing of infringement, irreparable harm may be presumed."); Wainright Sec., Inc., v. Wall Street Transcript Corp., 558 F.2d 91, 94 (2d Cir. 1977) (preliminary injunctions granted as a matter of course in copyright cases if prima facie case of copyright infringement can be shown because irreparable injury can be presumed when a copyright is infringed); Rushton v. Vitale, 218 F.2d 434, 436 (2d Cir. 1955) (same).

n284. A & M Records, Inc. v. Napster, Inc., 239 F.3d 1004 (9th Cir. 2001).

n285. The court noted:

We, however, briefly address Napster's First Amendment argument so that it is not reasserted on remand... . The company asserts two distinct free speech rights: (1) its right to publish a "directory' (here, the search index) and (2) its users' right to exchange information. We note that First Amendment concerns in copyright are allayed by the presence of the fair use doctrine... . There was a preliminary determination here that Napster users are not fair users. Uses of copyrighted material that are not fair uses are rightfully enjoined.

Id. at 1028 (citations omitted).

n286. 433 U.S. 562 (1977).

n287. Id. at 563-64.

n288. The Court explained:

The broadcast of a film of petitioner's entire act poses a substantial threat to the economic value of that performance. As the Ohio court recognized, this act is the product of petitioner's own talents and energy, the end result of much time, effort, and expense. Much of its economic value lies in the "right of exclusive control over the publicity given to his performance"; if the public can see the act free on television, it will be less willing to pay to see it at the fair. The effect of a public broadcast of the performance is similar to preventing petitioner from charging an admission fee. "The rationale for (protecting the right of publicity) is the straightforward one of preventing unjust enrichment by the theft of good will. No social purpose is served by having the defendant

get free some aspect of the plaintiff that would have market value and for which he would normally pay." Moreover, the broadcast of petitioner's entire performance, unlike the unauthorized use of another's name for purposes of trade or the incidental use of a name or picture by the press, goes to the heart of petitioner's ability to earn a living as an entertainer... .

Of course, Ohio's decision to protect petitioner's right of publicity here rests on more than a desire to compensate the performer for the time and effort invested in his act; the protection provides an economic incentive for him to make the investment required to produce a performance of interest to the public. This same consideration underlies the patent and copyright laws long enforced by this Court.

Id. at 575-76 (quoting Harry Kalven, Privacy in Tort Law - Were Warren and Brandeis Wrong?, 31 Law & Contemp. Probs. 326, 331 (1966).

n289. White v. Samsung Elecs. Am., Inc., 989 F.2d 1512, 1513 (9th Cir. 1993) (Kozinski, J., dissenting from order denying rehearing en banc.).

n290. 106 Cal. Rptr. 2d 126 (Cal. 2001), cert. denied, 122 S. Ct. 806 (2002).

n291. The right of publicity in California is both a statutory and a common law right. The statutory right originated in California Civil Code section 3344, enacted in 1971, which as originally enacted authorized recovery of damages by any living person whose name, photograph, or likeness has been used for commercial purposes without his or her consent. In 1979, the California Supreme Court recognized a common law right of publicity, which it described as a "complement" to the statutory cause of action. Lugosi v. Universal Pictures, 603 P.2d 425 (Cal. 1979). The court held, however, that because the common-law right was derived from the law of privacy, the cause of action did not survive the death of the person whose identity was exploited and was not descendible to his or her heirs or assignees. Id. at 428-29. In 1984, the California Legislature in effect overruled that aspect of Lugosi, creating a second statutory right of publicity that was descendible to the heirs and assignees of deceased persons. Cal. Civ. Code 990 (West 1998). In Comedy III Productions (the Three Stooges case) the California Supreme Court treated the 1984 statute as modeled on the previous 3344 and largely identical, but for the provisions extending the right beyond death. Section 990 reads in pertinent part:

Any person who uses a deceased personality's name, voice, signature, photograph, or likeness, in any manner, on or in products, merchandise, or goods, or for purposes of advertising or selling, or soliciting purchases of, products, merchandise, goods, or services, without prior consent ... shall be liable for any damages sustained by the person or persons injured as a result ... .

Cal. Civ. Code 990(a). The California statute defines "deceased personality" as a person "whose name, voice, signature, photograph, or likeness has commercial value at the time of his or her death," whether or not the

person actually used any of those features for commercial purposes while alive. 990(h). The statute expressly states that the rights it creates are "property rights" that are transferable before or after the personality dies, by contract or by trust or will. 990(b). The right to require consent terminates if there is neither transferee nor survivor, or 50 years after the personality dies. 990(e)-(g).

n292. The law contains a number of exemptions similar to the "fair use" defense in copyright, exempting use, for example, "in connection with any news, public affairs, or sports broadcast or account, or any political campaign," Cal. Civ. Code 990(j), as well as uses in "a play, book, magazine, newspaper, musical composition, film, radio or television program," 990(n)(1), a work of "political or newsworthy value," 990 (n)(2), and single and original "works of fine art," 990(n)(3).

n293. The bill was entitled "The Intelligence Authorization Act for Fiscal Year 2001." H.R. 4392, 106th Cong. (2000).

n294. See President William Jefferson Clinton, Message on Returning Without Approval to the House of Representatives the "Intelligence Authorization Act for Fiscal Year 2001," 36 Weekly Comp. Pres. Doc. 45 (Nov. 13, 2000).

n295. See, e.g., Editorial, The Leaks Veto, Wash. Post, Nov. 7, 2000, at A26; Ian Marquad, Veto Sets Example for Congress, The Quill, Dec. 1, 2000.

n296. In Snepp v. United States, 444 U.S. 507, 508 (1980), the Supreme Court reviewed the right of the United States to enforce an agreement by a former CIA employee, "that he would "not ... publish ... any information or material relating to the Agency, [or] its activities ... without specific prior approval by the Agency." Id. The ex-agent violated the agreement by publishing a book with some material relating to the CIA in it without securing CIA prior approval for such publication. The Supreme Court upheld the enforcement of the agreement, rejecting a First Amendment challenge.

n297. United States v. Morison, 844 F.2d 1057 (4th Cir. 1988).

n298. Even the dissenters in Bartnicki emphasized that this was not a leak by government agents of government material. Bartnicki v. Vopper, 532 U.S. 514, 546 (2001) (Rehnquist, C.J., dissenting).

n299. As the California Court of Appeals has explained:

Consequently, the news gathering component of the freedom of the press-the right to seek out information-is privileged at least to the extent it involves "routine ... reporting techniques." Such techniques, of course, include asking persons questions, including those with confidential or restricted information. While the government may desire to keep some proceedings confidential and may impose the duty upon participants to maintain confidentiality, it may not impose criminal or civil liability upon the press for obtaining and publishing newsworthy information through routine reporting techniques.

Nicholson v. McClatchy Newspapers, 223 Cal. Rptr. 58, 64 (Cal. Ct. App. 1986) (quoting Smith v. Daily Mail Publ'g Co., 443 U.S. 97, 103 (1979) and citing Landmark Communications, Inc. v. Virginia, 435 U.S. 829, 837-38 (1978)).

n300. Laurence H. Tribe, American Constitutional Law 965 (2d ed. 1988).

n301. Potter Stewart, Or of the Press, 26 Hastings L.J. 631, 636 (1975).

n302. See, e.g., Landmark Communications, Inc. v. Virginia, 435 U.S. 829, 845 (1978) (noting that much of the risk from disclosure of sensitive information regarding judicial disciplinary proceedings "can be eliminated through careful internal procedures to protect the confidentiality of Commission proceedings"); Okla. Publ'g Co. v. Dist. Ct., 430 U.S. 308, 311 (1977) (emphasizing trial court's failure to avail itself of the opportunity, provided by a state statute, to close juvenile hearing to the public); Cox Broad. Corp. v. Cohn, 420 U.S. 469, 496 (1975) ("If there are privacy interests to be protected in judicial proceedings, the States must respond by means which avoid public documentation or other exposure of private information.").

n303. In Boettger v. Loverro, 587 A.2d 712 (Pa. 1991), the appellant was charged with illegal gambling as a result of a police wiretap of phone conversations. A journalist was present in the courtroom during a hearing on a motion to suppress the information obtained in the wiretaps. When the hearing ended, a court clerk gave the reporter a file containing the transcript of the wiretaps. Following publication of the material, the appellant filed a civil action against the newspaper for violating a state wiretap statute proscribing the unlawful disclosure of wire communications. Applying Florida Star, the Supreme Court of Pennsylvania ultimately held that the First Amendment barred the prosecution, stating that "when the assistant district attorney filed a copy of the transcript with the Clerk of Courts, Criminal Division, it went in the public domain, irrespective of whether or not the action of the assistant district attorney was inadvertent." Id. at 718. In Florida Publishing Co. v. Brooke, 576 So. s2d 842 (Fla. Dist. Ct. App. 1991), a reporter came into possession of a letter written by a psychologist in a pending child dependency proceeding. The proceeding was closed to the public and the letter was classified by

law as not being a public record open to inspection. The trial judge issued an order restraining the reporter from disclosing the contents of the letter. Reversing the order on appeal, the court stated that "although a government may deny access to information and punish its theft, government may not prohibit or punish the publication of information once it falls into the hands of the press unless the need for secrecy is manifestly overwhelming." Id. at 846; see also Macon Tel. Publ'g Co. v. Tatum, 436 S.E.2d 655 (Ga. 1993) (applying Florida Star to preclude recovery by rape victim against a newspaper that had published her name after receiving it from police on the condition that it not be published without the victim's permission).

n304. This arms-length role of the press in our constitutional system was cogently summarized by Robert Kaiser, Managing Editor of The Washington Post, defending the Post's recent publication of material taken from a sealed deposition of President Clinton in the Paula Jones sexual harassment litigation:

This means, as some readers have pointed out to us, that we published Baker's story knowing that the information it contained was subject to Judge Wright's order. As a legal matter, such orders do not cover the media, and we and our lawyers believe that judges in America cannot gag the press, whose freedom is protected by the First Amendment to the Constitution. We expend much of our energy on finding information of public interest that others don't want published in a newspaper: That's what the Pentagon Papers case was about. And there are countless, more mundane examples. The District of Columbia's police department chronically withholds information we think belongs in the public domain; we are always battling the department to learn things it wants to hide from us. When we succeed, we publish it. We believe readers have a right to know.

Robert G. Kaiser, More About Our Sources and Methods, Wash. Post, Mar. 15, 1998, at C1.

n305. Alexander M. Bickel, The Morality of Consent 81 (1975).

n306. In New York Times Co. v. Sullivan, 376 U.S. 254 (1964), the plaintiff, L.B. Sullivan, was one of the three elected Commissioners of the City of Montgomery, Alabama. His duties included the supervision of the police department. Sullivan filed his suit on the basis of statements critical of police officials and their actions in relation to the civil rights movement and Dr. Martin Luther King, Jr. The United States Supreme Court held that evidence that Sullivan as Police Commissioner was the supervisory head of the Police Department was constitutionally insufficient to show that the statements about police activity were "of and concerning" him. The Court rejected as inconsistent with the United States Constitution the proposition that "in measuring the performance or deficiencies of groups, praise or criticism is usually attached to the official in complete control of the body." Id. at 263. To allow the jury to connect the statements with Sullivan on such a presumption alone was, in the Supreme Court's view, to permit prosecutions for libel on government, which the United States Constitution does not tolerate. Id. at 273-76. "Such a proposition," the Court instructed, "may not constitutionally be utilized to establish that an otherwise impersonal attack on governmental operations was a libel of an official responsible for those operations." Id. at 292. These principles were reiterated and reinforced by the Supreme Court in Rosenblatt v. Baer, 383 U.S. 75, 82 (1966), in which the Court refused to accept, as constitutionally sufficient, a theory that a cause of action could be maintained against a publication that cast "indiscriminate suspicion" on members of a group who were allegedly responsible for the conduct of a county

ski recreation area, for this was "to invite the spectre of prosecutions for libel on government, which the Constitution does not tolerate in any form... . "Such a proposition may not constitutionally be utilized to establish that an otherwise impersonal attack on governmental operations was a libel of an official responsible for those operations.'" Id. at 81 (citations omitted) (quoting Sullivan, 376 U.S. at 292).

n307. See supra text accompanying notes 102, 196-198, 224-241.

n308. The one caveat to the division suggested here involves situations in which the press or its representatives are in some direct way parties to an official proceeding, and subjected to generally applicable laws imposing norms of confidentiality in relation to those proceedings. A news organization that is an actual party to civil litigation may, like any other litigant, be subjected to protective orders limiting dissemination of material obtained through discovery. See Seattle Times Co. v. Rhinehart, 467 U.S. 20 (1984) (sustaining protective order against newspaper defendant in libel suit from publishing information obtained in discovery). In Seattle Times, the Court applied intermediate scrutiny, noting that the protective order was based on the means through which the information in question had been obtained - namely, through the compulsory judicial processes created by discovery rules - observing that "the party may disseminate the identical information ... as long as the information is gained through [other] means." Id. at 34. But when sealed court documents fall into the hands of journalists who are not parties to a suit and directly subject to any protective order, the First Amendment balance is normally understood as being quite different. See Procter & Gamble Co. v. Bankers Trust Co., 78 F.3d 219, 225 (6th Cir. 1996) ("Seattle Times holds that parties to civil litigation do not have a right to disseminate information they have gained through participation in the discovery process. That case, however, does not govern the situation where an independent news agency, having gained access to sealed documents, decides to publish them."). Similarly, while the Supreme Court has applied strict scrutiny to place limits on the extent to which the government may enforce secrecy requirements relating to grand jury proceedings, see Butterworth v. Smith, 494 U.S. 624, 631 (1990), the Court appears to distinguish between rules that gag a grand jury witness from repeating information acquired by the witness outside the grand jury and then furnished to the grand jury during testimony, and information that the witness acquires inside the grand jury, having been exposed to it only because the witness was brought into the grand jury process. Id. at 631-32 (explaining that the principles of Seattle Times would have been applicable had the statute prohibited disclosure only of information "obtained as a result of ... participation in the proceedings of the grand jury").

n309. 128 F.3d 233 (4th Cir. 1997), cert. denied, 523 U.S. 1074 (1998). The author represented the plaintiffs in this litigation. The story of the litigation is told in Rod Smolla, Deliberate Intent: A Lawyer Tells the True Story of Murder by the Book (1999).

n310. 273 F.3d 429 (2d Cir. 2001). The author of this article wrote an amicus brief in the Second Circuit supporting the copyright holders' position in the litigation.

n311. See generally Smolla, supra note 309.

n312. Rice, 128 F.3d at 247.

n313. 395 U.S. 444 (1969).

n314. Id. at 447.

n315. 17 U.S.C.A. 1201 (West Supp. 2001).

n316. Unlike copies made from an analog source, which degrade when data or digital data is copied or transmitted, there is little or no quality degradation.

n317. Title 17 U.S.C.A. 1201(a)(2) (1999) provides:

no person shall manufacture, import, offer to the public, provide, or otherwise traffic in any technology, product, service, device, component, or part thereof, that

(A)is primarily designed or produced for the purpose of circumventing a technological measure that effectively controls access to a work protected under this title;

(B)has only limited commercially significant purpose or use other than to circumvent a technological measure that effectively controls access to a work protected under this title; or

(C)is marketed by that person or another acting in concert with that person with that person's knowledge for use

in circumventing a technological measure that effectively controls access to a work protected under this title.

Id.

n318. See Smolla, supra note 309. In a dissenting opinion in Dennis v. United States, Justice Douglas noted:

If this were a case where those who claimed protection under the First Amendment were teaching the techniques of sabotage, the assassination of the President, the filching of documents from public files, the planting of bombs, the art of street warfare, and the like, I would have no doubts. The freedom to speak is not absolute; the teaching of methods of terror and other seditious conduct should be beyond the pale ... .

Dennis v. United States, 341 U.S. 494, 581 (1951) (Douglas, J., dissenting).

n319. Rice v. Paladin Enters., Inc., 128 F.3d 233, 267 (1997).

n320. See Cable/Home Communication Corp. v. Network Prods., Inc., 902 F.2d 829, 849 (11th Cir. 1990) (finding that promotion of statutorily-prohibited "descrambling devices" for subscription cable television programming, and sale of pirated computer chips to compromise the encryption of plaintiffs' transmissions, were not protected by the First Amendment); Cal. Satellite Sys. v. Seimon, 767 F.2d 1364, 1367-68 (9th Cir. 1985) (finding no First Amendment right to pirate scrambled satellite broadcast signals).

n321. See Goldstein v. California, 412 U.S. 546, 562 (1973) ("As our technology has expanded the means available for creative activity and has provided economical means for reproducing manifestations of such activity, new areas of federal protection have been initiated.").

n322. See 17 U.S.C.A. 1201(f)(2), (f)(3), (g)(4), (j)(4) (West Supp. 2001) (creating exceptions for such purposes as reverse engineering, encryption research, and security testing).

n323. See supra note 196 and accompanying text.

n324. See United States v. Bodin, 375 F. Supp. 1265, 1267 (W.D. Okla. 1974) ("We do not find any denial

of freedom of expression to the "tape pirate.' What he seeks is not the freedom to express himself artistically or otherwise, but the right to make exact and identical copies of sound recordings produced by others.").

n325. The fair user can make a compilation from tapes. Or the fair user can show an excerpt from a film on a DVD, then pop out the disk (or rotate disks in a typical multidisk DVD player) to show an excerpt from the next film. Film lecturers and movie critiques have managed to survive the first century of film criticism without DVD machines.

n326. See United States v. Thomas, 116 F.3d 606, 614-15 (2d Cir. 1997) (while jury nullification "may at times manifest itself as a form of civil disobedience that some may regard as tolerable," in a nation committed to the rule of law such civil disobedience is not a "right").

TAB 18

1 of 1 DOCUMENT

Restatement of the Law, Second, Torts

Case Citations

Rules and Principles

Division 1 - Intentional Harms to Persons, Land, and Chattels

Chapter 5 - Arrest and Prevention of Crime

Topic 1 - Arrest

Title B - Conditions of the Privilege

5 - Assisting Third Person to Make Arrest

Restat 2d of Torts, § 139

§ 139 When Third Person Privileged

(1) The actor is privileged to use force against another for the purpose of assisting a third person to make or maintain an arrest or re-arrest if the third person is himself privileged to make the arrest.
(2) The actor is not privileged to use force against another for the purpose of assisting a third person to make an arrest which the third person is not himself privileged to make, unless the actor is assisting a peace officer at the officer's request in making the arrest for a criminal offense and the actor is not convinced that the officer is not privileged to make it.

CAVEAT: Caveat:

The Institute expresses no opinion as to whether there is a privilege to assist a peace officer without the latter's request, if the officer has no opportunity to ask for the actor's assistance and the actor reasonably believes that his assistance is necessary to effect the arrest, in a situation in which the peace officer is not himself privileged, but the actor is ignorant of such fact.

COMMENTS & ILLUSTRATIONS: Comment:

a. This Section deals only with the privilege conferred upon an actor by the fact that he is assisting a third person in effecting an arrest or recapture of the other, or in maintaining a third person's custody of the other. If the circumstances are such that the actor is himself privileged to make the arrest irrespective of the third person's request, as where a felony has been committed and the actor reasonably suspects the other of having committed it, his privilege is not affected by the fact that he is assisting a private person, or a peace officer, who does not reasonably suspect the other and who, therefore, is not privileged to arrest him.

Comment on Subsection (1):

b. The situations to which the statement in this Subsection apply are the following:

1. The actor assists a private individual in making an arrest, with or without a warrant, either for a criminal offense or under a warrant issued in civil proceedings.

2. The actor assists a peace officer in making an arrest under a warrant issued in civil proceedings.

3. The actor assists a peace officer in making an arrest for a criminal offense without any request of the officer, who has an opportunity to ask for assistance, or who has no opportunity to ask for assistance, the circumstances being such that the actor has reason to believe that the officer cannot make the arrest without his assistance.

c. The statement in this Subsection not only protects the actor from liability for the force used against the other in assisting the officer, but also precludes the existence of any privilege on the part of the other to resist the actor's use of reasonable force in his effort to effect the arrest.

Comment on Subsection (2):

d. The interest of society in the apprehension of offenders and in the investigation of crime makes it the duty of all persons, upon request, to assist a peace officer in making an arrest, unless there is no doubt that the arrest is unprivileged and tortious. Even a reasonable suspicion or belief that the arrest is unprivileged is not enough to relieve a citizen from the duty of assisting the officer. The officer's need for assistance often arises in a sudden emergency and the assistance must be given at once to be effective. To require a person whom a peace officer calls upon to assist in making an arrest to take the risk of being liable in the event that the officer is not himself privileged to make it, unless such person exercises such judgment and makes such investigations as he would be required to make were he acting on his own initiative, would seriously deter such persons from giving the prompt aid necessary to effect arrests which, save in an insignificant minority of cases, the officer is privileged to make. Therefore, the actor is privileged to rely upon the officer's request and assist him unless the facts are such that the actor knows or is convinced beyond a reasonable doubt that the officer is not himself privileged to make the arrest. Thus, the actor is privileged upon a peace officer's request to assist him in arresting another without a warrant for a past felony unless the actor knows or is convinced beyond a reasonable doubt that the officer's suspicion is unreasonable. So too, if a peace officer requests the actor to assist him in making an arrest under a warrant for a crime, the actor is privileged to do so without being required to inspect the warrant to determine its sufficiency, or even to satisfy himself that the officer has a warrant in his possession. Therefore, unless the actor reads the warrant, the service of which he is asked to assist, he is not affected by any defect in the warrant, no matter how obvious.

On the other hand, no one is required or privileged to assist an officer in making an arrest which he knows that the officer is not privileged to make. Thus, the actor is not privileged to assist an officer in making an arrest if he knows or is convinced beyond a reasonable doubt that the suspicion upon which the officer is arresting for a felony is unreasonable, or that a warrant which the officer is attempting to serve is on its face invalid, or that the person whom the officer is seeking to arrest under the warrant is not sufficiently named or described therein.

e. If a peace officer requests the actor to assist him in making an arrest with or without a warrant, the actor is privileged to comply, irrespective of whether he has or has not reason to believe that his assistance is necessary to make the arrest. It is for the peace officer and not the actor to determine the necessity for assistance.

f. The statement in Subsection (2) protects the actor from liability although he is assisting an officer who is not privileged to make the arrest and who is, therefore, himself liable to the person arrested for any force which he, the officer, uses in making the arrest. It does not, however, preclude the existence of a privilege in the other to resist the actor's attempt to make the arrest. If the officer is not privileged to make the arrest, the other is privileged to use such force as is reasonably necessary to prevent his arrest against those, whether the officer or his assistants, who are trying to arrest him.

CROSS REFERENCES: ALR Annotations:

Liability of a private person answering call of known or asserted peace or police officer to assist in making arrest which turns out to be unlawful. 29 A.L.R.2d 825.

TAB 19

LEXSTAT REST 2D TORTS 652B

Restatement of the Law, Second, Torts

Case Citations

Rules and Principles

Division 6A - Privacy

Chapter 28A - Invasion of Privacy

Restat 2d of Torts, § 652B

§ 652B Intrusion Upon Seclusion

One who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person.

COMMENTS & ILLUSTRATIONS: Comment:

a. The form of invasion of privacy covered by this Section does not depend upon any publicity given to the person whose interest is invaded or to his affairs. It consists solely of an intentional interference with his interest in solitude or seclusion, either as to his person or as to his private affairs or concerns, of a kind that would be highly offensive to a reasonable man.

b. The invasion may be by physical intrusion into a place in which the plaintiff has secluded himself, as when the defendant forces his way into the plaintiff's room in a hotel or insists over the plaintiff's objection in entering his home. It may also be by the use of the defendant's senses, with or without mechanical aids, to oversee or overhear the plaintiff's private affairs, as by looking into his upstairs windows with binoculars or tapping his telephone wires. It may be by some other form of investigation or examination into his private concerns, as by opening his private and personal mail, searching his safe or his wallet, examining his private bank account, or compelling him by a forged court order to permit an inspection of his personal documents. The intrusion itself makes the defendant subject to liability, even though there is no publication or other use of any kind of the photograph or information outlined.

Illustrations:

1. A, a woman, is sick in a hospital with a rare disease that arouses public curiosity. B, a newspaper reporter, calls her on the telephone and asks for an interview, but she refuses to see him. B then goes to the hospital, enters A's room and over her objection takes her photograph. B has invaded A's privacy.

2. A, a private detective seeking evidence for use in a lawsuit, rents a room in a house adjoining B's residence, and for two weeks looks into the windows of B's upstairs bedroom through a telescope taking intimate pictures with a telescopic lens. A has invaded B's privacy.

3. The same facts as in Illustration 2, except that A taps B's telephone wires and installs a recording device to make a record of B's conversations. A has invaded B's privacy.

4. A is seeking evidence for use in a civil action he is bringing against B. He goes to the bank in which B has his

personal account, exhibits a forged court order, and demands to be allowed to examine the bank's records of the account. The bank submits to the order and permits him to do so. A has invaded B's privacy.

5. A, a professional photographer, seeking to promote his business, telephones B, a lady of social prominence, every day for a month, insisting that she come to his studio and be photographed. The calls are made at meal times, late at night and at other inconvenient times, and A ignores B's requests to desist. A has invaded B's privacy.

c. The defendant is subject to liability under the rule stated in this Section only when he has intruded into a private place, or has otherwise invaded a private seclusion that the plaintiff has thrown about his person or affairs. Thus there is no liability for the examination of a public record concerning the plaintiff, or of documents that the plaintiff is required to keep and make available for public inspection. Nor is there liability for observing him or even taking his photograph while he is walking on the public highway, since he is not then in seclusion, and his appearance is public and open to the public eye. Even in a public place, however, there may be some matters about the plaintiff, such as his underwear or lack of it, that are not exhibited to the public gaze; and there may still be invasion of privacy when there is intrusion upon these matters.

Illustrations:

6. A is drunk on the public street. B takes his photograph in that condition. B has not invaded A's privacy.

7. A, a young woman, attends a "Fun House," a public place of amusement where various tricks are played upon visitors. While she is there a concealed jet of compressed air blows her skirts over her head, and reveals her underwear. B takes a photograph of her in that position. B has invaded A's privacy.

d. There is likewise no liability unless the interference with the plaintiff's seclusion is a substantial one, of a kind that would be highly offensive to the ordinary reasonable man, as the result of conduct to which the reasonable man would strongly object. Thus there is no liability for knocking at the plaintiff's door, or calling him to the telephone on one occasion or even two or three, to demand payment of a debt. It is only when the telephone calls are repeated with such persistence and frequency as to amount to a course of hounding the plaintiff, that becomes a substantial burden to his existence, that his privacy is invaded.

Illustration:

8. A, a landlord, calls upon B, his tenant, at nine o'clock on Sunday morning, to demand payment of the rent, although he knows that B is not ready to pay it and that B objects to such a visit on Sunday. B is seriously annoyed. This is not an invasion of B's privacy.

REPORTERS NOTES: This Section is new.

Comment b: As to physical intrusion, see Dietemann v. Time, Inc., 449 F.2d 245 (9 Cir. 1971); Thompson v. City of Jacksonville, 130 So.2d 105 (Fla.App.1961) (search of home without warrant); Byfield v. Candler, 33 Ga.App. 275, 125 S.E. 905 (1924) (breaking into woman's bedroom on a steamboat); Young v. Western & Atlantic R. Co., 39 Ga.App. 761, 148 S.E. 414 (1929) (search of home without a warrant); De May v. Roberts, 46 Mich. 160, 9 N.W. 146 (1881) (intruding upon childbirth); Welsh v. Pritchard, 125 Mont. 517, 241 P.2d 816 (1952) (landlord moving in on tenant); Sutherland v. Kroger Co., 144 W.Va. 673, 110 S.E.2d 716 (1959) (illegal search of woman's shopping bag in a store).

Consent to enter need not be express. See Vespa v. Safety Federal Sav. & Loan Ass'n, 219 Kan. 578, 549 P.2d 878 (1976). In Ford Motor Co. v. Williams, 108 Ga.App. 21, 132 S.E.2d 206 (1963), liability was found when the defendant entered the plaintiff's home, even though no one was there at the time. See also Gonzalez v. Southwestern Bell Tel. Co., 555 S.W.2d 219 (Tex. Civ.App.1977) (phone removed when deposit was not paid).

Illustration 1 is based upon Barber v. Time Inc., 348 Mo. 1199, 159 S.W.2d 291 (1942).

See also Noble v. Sears, Roebuck & Co., 33 Cal.App.3d 654, 109 Cal.Rptr. 269 (1973) (entry into hospital room by deception); Love v. Southern Bell Tel. & Tel. Co., 263 So.2d 460 (La.App.1972) refused, 262 La. 1117, 266 So.2d 429 (plaintiff photographed at home, drunk); Estate of Berthiaume v. Pratt, 365 A.2d 792 (Me.1976) (doctor photographed dying patient over protests).

Illustration 2 is based upon Souder v. Pendleton Detectives, 88 So.2d 716 (La.App.1956).

See also Pritchett v. Board of Commissioners of Knox County, 42 Ind.App. 3, 85 N.E. 32 (1908); Moore v. New York Elevated R. Co., 130 N.Y. 523, 29 N.E. 997 (1892).

On opening of mail, see Brinbaum v. United States, 436 F. Supp. 967 (S.D.N.Y.1977); Vernars v. Young, 539 F.2d 966 (3 Cir. 1976).

On reasonable investigation of the plaintiff's claim, see Alabama Elec. Coop., Inc. v. Partridge, 284 Ala. 442, 225 So.2d 848 (1969); Tucker v. American Employers' Ins. Co., 171 So.2d 437 (Fla.App. 1965); Forster v. Manchester, 410 Pa. 192, 189 A.2d 147 (1963); Shorter v. Retail Credit Co., 251 F.Supp. 329 (D.S.C. 1966); cf. Bodrey v. Cape, 120 Ga.App. 859, 172 S.E.2d 643 (1969); Ellenburg v. Pinkerton's, Inc., 125 Ga.App. 648, 188 S.E.2d 911 (1972) appeal after remand, 130 Ga.App. 254, 202 S.E.2d 701; Payne v. Lauglin, 486 S.W.2d 192 (Tex.Civ.App.1972).

But ostentatious "rough shadowing" was held actionable in Pinkerton Nat. Detective Agency v. Stevens, 108 Ga.App. 159, 132 S.E.2d 119 (1963).

Illustration 3 is based upon Rhodes v. Graham, 238 Ky. 225, 37 S.W.2d 46 (1931).

See also McDaniel v. Atlanta Coca Cola Bottling Co., 60 Ga. App. 92, 2 S.E.2d 810 (1939); Elson v. Bowen, 83 Nev. 515, 436 P.2d 12 (1967); Le Crone v. Ohio Bell Tel. Co., 120 Ohio App. 129, 201 N.E.2d 533 (1963); Roach v. Harper, 143 W.Va. 869, 105 S.E.2d 564 (1958).

The information obtained need not be used. Fowler v. Southern Bell Tel. & Tel. Co., 343 F.2d 150 (5 Cir. 1965); cf. Corcoran v. Southwestern Bell Tel. Co., 572 S.W.2d 212 (Mo.App.1978) (no publication required).

In Hamberger v. Eastman, 106 N.H. 107, 206 A.2d 239 (1964), the installation of a listening device in a bedroom was held to be an invasion of privacy, even though nothing was overheard.

There was no liability in Simmons v. Southwestern Bell Tel. Co., 452 F.Supp. 392 (W.D.Okl. 1978) (monitoring special line not to be used for private calls).

On recording by one party to a telephone conversation, see Martin v. De Silva, 566 F.2d 361 (1 Cir. 1977); Matter of Bates, 555 S.W.2d 420 (Tex.1977).

Illustration 4 is based upon Brex v. Smith, 104 N.J.Eq. 386, 146 A. 34 (1929); Zimmerman v. Wilson, 81 F.2d 847 (3 Cir. 1936); Frey v. Dixon, 141 N.J.Eq. 481, 58 A.2d 86 (1948) (invalid court order for production of documents); State ex rel. Clemens v. Witthaus, 360 Mo. 274, 228 S.W. 2d 4 (1950) (same); cf. Bednarik v. Bednarik, 18 N.J.Misc. 633, 16 A.2d 80 (1940) (unauthorized compulsory blood test).

Locating and supplying information for one's own files is not an intrusion. Tureen v. Equifex, Inc., 571 F.2d 411 (8 Cir. 1978); cf. Munley v. ISC Financial House, Inc., 584 P.2d 1336 (Okl. 1978) (asking questions of neighbors).

Illustration 5 is based upon Housh v. Peth, 165 Ohio St. 35, 133 N.E.2d 340 (1956).

See also Galella v. Onassis, 487 F.2d 986 (2 Cir. 1973); Harms v. Miami Daily News, 127 So.2d 715

(Fla.App.1961); Carey v. Statewide Finance Co., 3 Conn.Cir. 716, 223 A.2d 405 (1966); cf. Wiggins v. Moskins Credit Clothing Store, 137 F.Supp. 764 (E.D. S.C.1956) (goes on nuisance); Robbins v. Canadian Broadcasting Co., 12 Dom.L.Rep.2d 35 (1958).

Comment c: Illustration 6 is based upon Gill v. Hearst Pub. Co., 40 Cal.2d 224, 253 P.2d 441 (1953) (embracing wife in public market); DeLury v. Kretchmer, 66 Misc.2d 897, 322 N.Y.S.2d 517 (1971).

See also Berg v. Minneapolis Star & Tribune Co., 79 F.Supp. 957 (D.Minn.1948) (courtroom); Travers v. Paton, 261 F.Supp. 110 (D.Conn.1966) (same); Lyles v. State, 330 P.2d 734 (Okl.Cr.1958) (same); Man v. Warner Bros., 317 F.Supp. 50 (S.D.N.Y.1970) (musician on stage at Woodstock rock festival); Gautier v. Pro-Football, Inc., 304 N.Y. 354, 107 N.E.2d 485 (1952); Forster v. Manchester, 410 Pa. 192, 189 A.2d 147 (1963).

In United States v. Gugel, 119 F.Supp. 897 (E.D.Ky.1954), the right to take the pictures and publish them was said to be guaranteed by the Constitution of the United States.

Illustration 7 is taken from Daily Times Democrat v. Graham, 276 Ala. 380, 162 So.2d 474 (1964).

Compare Neff v. Time, Inc., 406 F.Supp. 858 (W.D.Pa.1976) (picture of football player taken with his consent, but without his knowledge that his fly was open).

As to public records, see Rome Sentinel Co. v. Boustedt, 43 Misc.2d 598, 252 N.Y.S.2d 10 (1964).

Comment d: Illustration 8 is taken from Horstman v. Newman, 291 S.W.2d 567 (Ky.1956).

In accord is Harms v. Miami Daily News, Inc., 127 So.2d 715 (Fla.App.1961) (for jury whether telephone calls objectionable to a reasonable person).

Other cases holding that the intrusion must be highly offensive to a reasonable person. Froelich v. Werbin, 219 Kan. 461, 548 P.2d 482 (1976); Everett v. Carvel Corp., 70 Misc.2d 734, 334 N.Y.S. 2d 922 (1972); Munley v. ISC Financial House, Inc., 584 P.2d 1336 (Okl.1978); McLain v. Boise Cascade Corp., 271 Or. 549, 533 P.2d 343 (1975).

Unsolicited mailings do not constitute an actionable intrusion. Stilson v. Reader's Digest Ass'n, 28 Cal.App.3d 270, 104 Cal.Rptr. 581 (1972) (sweepstakes advertisement for subscriptions); Bradshaw v. Michigan Nat. Bank, 39 Mich.App. 354, 197 N.W.2d 531 (1971) (credit card).

Solicitation on a public street by a political canvasser is not actionable. City of Bowling Green v. Lodico, 11 Ohio St.2d 135, 228 N.E.2d 325 (1967).

See Ezer, Intrusion on Solitude, 21 Law in Transition (1961); Note, The Emerging Tort of Intrusion, 55 Iowa L.Rev. 718 (1970); Notes, 5 Ark.L.Rev. 388 (1951), 57 Geo.L.J. 509 (1969), 17 Vand.L.Rev. 1342 (1964).

CROSS REFERENCES: ALR Annotations:

Invasion of privacy by use of a picture of plaintiff's property for advertising purposes. 87 A.L.R.3d 1279.
Taking unauthorized photographs as invasion of privacy. 86 A.L.R.3d 374.
Invasion of privacy by sale or rental of list of customers, subscribers, or the like, to one who will use it for advertising purposes. 82 A.L.R.3d 772.
Unsolicited mailing, distribution, house call, or telephone call as invasion of privacy. 56 A.L.R.3d 457.
Uninvited entry into another's living quarters as invasion of privacy. 56 A.L.R.3d 434.
Invasion of privacy by radio or television. 56 A.L.R.3d 386.
Investigations and surveillance, shadowing and trailing, as violation of right of privacy. 13 A.L.R.3d 1025.
Eavesdropping as violating right of privacy. 11 A.L.R.3d 1296.

Digest System Key Numbers:

Torts 8.5

TAB 20

1 of 1 DOCUMENT

The Washington Post
washingtonpost.com
The Washington Post

December 23, 2005 Friday
Final Edition

SECTION: Editorial; A21

LENGTH: 773 words

HEADLINE: Power We Didn't Grant

BYLINE: Tom Daschle

BODY:

In the face of mounting questions about news stories saying that President Bush approved a program to wiretap American citizens without getting warrants, the White House argues that Congress granted it authority for such surveillance in the 2001 legislation authorizing the use of force against al Qaeda. On Tuesday, Vice President Cheney said the president "was granted authority by the Congress to use all means necessary to take on the terrorists, and that's what we've done."

As Senate majority leader at the time, I helped negotiate that law with the White House counsel's office over two harried days. I can state categorically that the subject of warrantless wiretaps of American citizens never came up. I did not and never would have supported giving authority to the president for such wiretaps. I am also confident that the 98 senators who voted in favor of authorization of force against al Qaeda did not believe that they were also voting for warrantless domestic surveillance.

On the evening of Sept. 12, 2001, the White House proposed that Congress authorize the use of military force to "deter and pre-empt any future acts of terrorism or aggression against the United States." Believing the scope of this language was too broad and ill defined, Congress chose instead, on Sept. 14, to authorize "all necessary and appropriate force against those nations, organizations or persons [the president] determines planned, authorized, committed or aided" the attacks of Sept. 11. With this language, Congress denied the president the more expansive authority he sought and insisted that his authority be used specifically against Osama bin Laden and al Qaeda.

Just before the Senate acted on this compromise resolution, the White House sought one last change. Literally minutes before the Senate cast its vote, the administration sought to add the words "in the United States and" after "appropriate force" in the agreed-upon text. This last-minute change would have given the president broad authority to exercise expansive powers not just overseas -- where we all understood he wanted authority to act -- but right here in the United States, potentially against American citizens. I could see no justification for Congress to accede to this extraordinary request for additional authority. I refused.

The shock and rage we all felt in the hours after the attack were still fresh. America was reeling from the first attack on our soil since Pearl Harbor. We suspected thousands had been killed, and many who worked in the World Trade Center and the Pentagon were not yet accounted for. Even so, a strong bipartisan majority could not agree to the administration's request for an unprecedented grant of authority.

The Bush administration now argues those powers were inherently contained in the resolution adopted by Congress -- but at the time, the administration clearly felt they weren't or it wouldn't have tried to insert the additional language.

All Americans agree that keeping our nation safe from terrorists demands aggressive and innovative tactics. This unity was reflected in the near-unanimous support for the original resolution and the Patriot Act in those harrowing days after Sept. 11. But there are right and wrong ways to defeat terrorists, and that is a distinction this administration has never seemed to accept. Instead of employing tactics that preserve Americans' freedoms and inspire the faith and confidence of the American people, the White House seems to have chosen methods that can only breed fear and suspicion.

If the stories in the media over the past week are accurate, the president has exercised authority that I do not believe is granted to him in the Constitution, and that I know is not granted to him in the law that I helped negotiate with his counsel and that Congress approved in the days after Sept. 11. For that reason, the president should explain the specific legal justification for his authorization of these actions, Congress should fully investigate these actions and the president's justification for them, and the administration should cooperate fully with that investigation.

In the meantime, if the president believes the current legal architecture of our country is insufficient for the fight against terrorism, he should propose changes to our laws in the light of day.

That is how a great democracy operates. And that is how this great democracy will defeat terrorism.

The writer, a former Democratic senator from South Dakota, was Senate majority leader in 2001-02. He is now distinguished senior fellow at the Center for American Progress.

LOAD-DATE: December 23, 2005