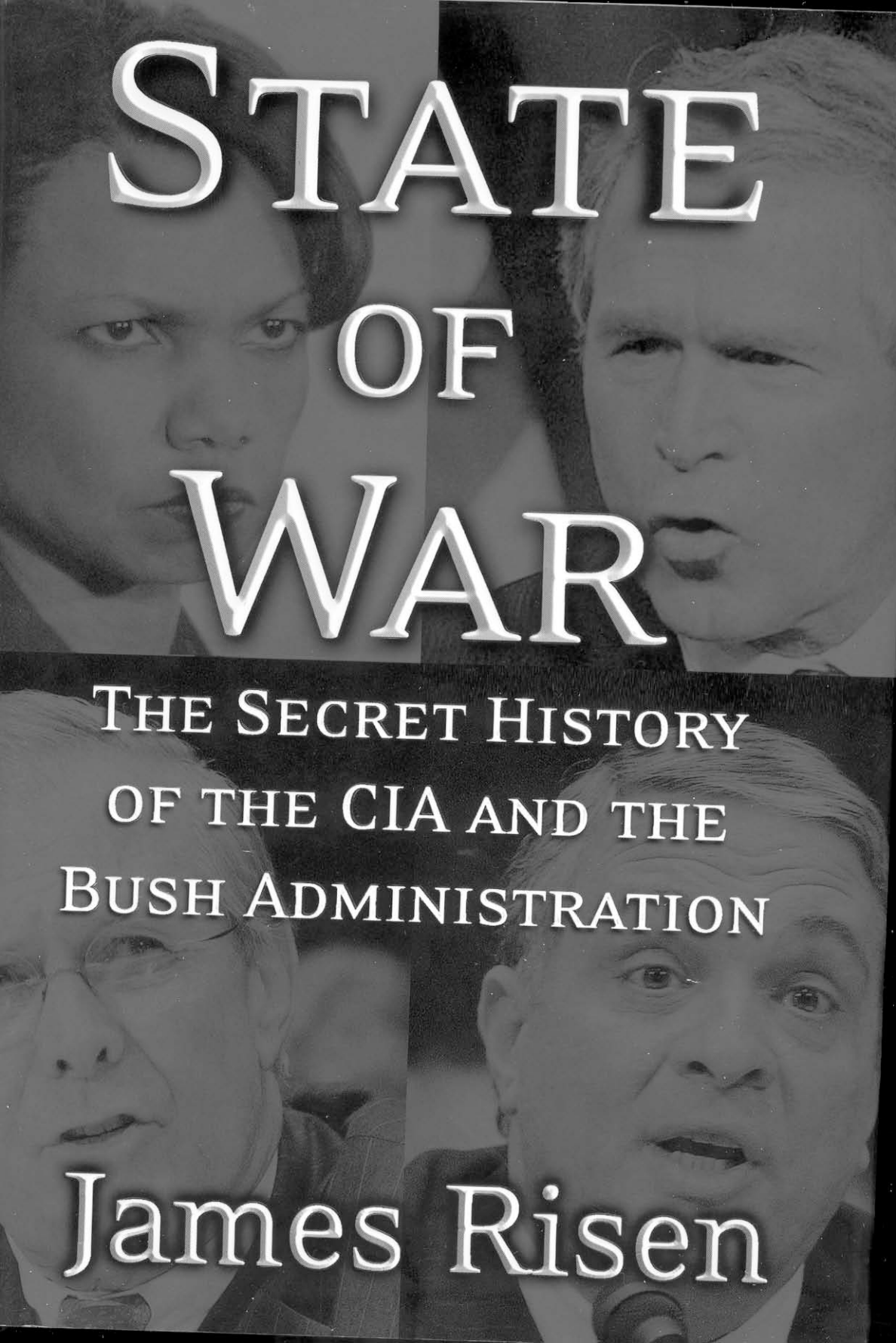
STATE
OF
WAR
THE SECRET HISTORY
OF THE CIA AND THE
BUSH ADMINISTRATION
James Risen

*f*P
FREE PRESS
A Division of Simon & Schuster, Inc.
1230 Avenue of the Americas
New York, NY 10020

Designed by Dana Sloan

Manufactured in the United States of America

10 9 8 7 6 5 4 3 2 1

Library of Congress Cataloging-in-Publication Data is available.

ISBN-13: 978-0-7432-7066-3
ISBN-10: 0-7432-7066-5

For information regarding special discounts for bulk purchases,
please contact Simon & Schuster Special Sales at 1-800-456-6798
or business@simonandschuster.com

2

THE PROGRAM

IN FEBRUARY 1999, Michael Hayden, a balding and soft-spoken air force lieutenant general from Pennsylvania, was nominated by President Bill Clinton to become the director of the National Security Agency, the largest organization in the United States intelligence community, double the size of the CIA and truly the dominant electronic spy service in the world. For Hayden, a military intelligence officer who had begun his career as an analyst at the Strategic Air Command at the height of the Cold War, the new assignment was the great reward for nearly thirty years of hard slogging up the chain of command, for persistence in a career that Hayden must have at some point considered a dead end, particularly after a four-year assignment in the 1970s in the most obscure corner of the air force, as an ROTC instructor at tiny St. Michael's College in Winooski, Vermont.

Hayden was stationed in South Korea, serving in a senior staff position, when this big promotion came. Coincidentally, Hollywood had just released a movie about the NSA, and it was showing in Korea as Hayden was preparing for his new assignment. Mike Hayden couldn't resist going to see Will Smith and Gene Hackman in *Enemy of the State.*

Hayden was appalled. The movie showed the NSA as an evil, rogue organization that used its cutting-edge technology to spy on

and persecute unwitting Americans. After thoroughly penetrating every aspect of his life, an NSA team of assassins tries to kill Will Smith, who plays a Washington lawyer whom the NSA bosses suspect knows too much about the agency's dark side. Smith is saved only after he befriends Gene Hackman, playing a reclusive former NSA technical wizard who turns the tables on the agency and helps Smith get the truth out.

The film's message—that the NSA is an uncontrollable beast run by a cadre of ruthless bureaucrats secretly trampling on the civil rights of Americans—sent shivers through Hayden. *Enemy of the State* was one of the most prominent movies ever made about the NSA, and it reinforced every dark nightmare the American public had about the government's supersecret eavesdropping and code-breaking apparatus.

The movie came out just as a controversy over the NSA was breaking out in Europe as well, thanks to the agency's global surveillance programs, known publicly as Echelon, through which it vacuums up communications around the world outside the United States. European politicians (outside of the United Kingdom, where the Government Communications Headquarters, GCHQ, Britain's version of the NSA, cooperates with U.S. eavesdropping operations) were bitter that the United States was targeting its giant eavesdropping machinery at them, and their anger prompted some Americans to wonder whether Echelon was ever turned on inside the United States for use against political dissidents. The Electronic Privacy Information Center, a Washington group that tries to keep up with NSA activities, went to court to try to discover whether Echelon or similar programs were being used to spy on Americans.

For an intelligence bureaucrat, Hayden responded to the controversies over *Enemy of the State* and Echelon in an unorthodox and creative way. Instead of denying the film's cultural influence, or the growing public uneasiness over NSA's power, he realized that his agency had to open itself up to greater scrutiny in order to disprove

the conspiracy theorists. The NSA, whose very existence had once been a state secret, had to start talking about itself, and it had to start dealing with the press.

This was unprecedented for the NSA, and it was disorienting and shocking for the agency's old hands, who had been trained never, ever, to discuss their jobs, even with their husbands or wives. The NSA was, at heart, a blue-collar spy agency. It operated the intelligence plumbing, and so it tended to attract quiet technicians, math and linguistics geeks, and military and civilian managers who were bureaucratic conformists. None of them understood Hayden's desire to deal with the outside world, let alone the press. They knew that the public image of the NSA was a badly distorted cartoon, and they also knew that the agency had actually accomplished remarkable—and politically risky—things on behalf of the United States, almost none of which had ever become public.

For example, in 1990 the CIA and NSA jointly stole virtually every code machine (and their manuals) in use by the Soviet Union, giving NSA's code breakers a remarkable advantage on Moscow. The CIA and NSA obtained the Soviet code machines in Prague and then flew them to NSA headquarters at Fort Meade, Maryland, to be carefully dissected. The operation was an espionage triumph, but one that NSA officials would never consider discussing publicly, even many years later. Better to let public misunderstandings about NSA fester, the old-timers believed, than to disclose the agency's successes.

But if NSA didn't start talking, Hayden feared, then urban legends about the agency would take hold in the national imagination, and support for it and its mission would erode. "I made the judgment that we couldn't survive with the popular impression of this agency being formed by the last Will Smith movie," Hayden told CNN. The agency, Hayden promised, had learned its lesson from the dark days of the 1970s, when the domestic abuses of the FBI, the CIA—and the NSA—were revealed by congressional committees chaired by Idaho

senator Frank Church and New York congressman Otis Pike. Church and Pike discovered that the NSA had been involved, along with the FBI, in domestic spying on activists in the civil rights and anti–Vietnam War movements.

The NSA had been created in 1952 by President Harry Truman in order to consolidate the government's code-breaking and code-making capabilities, and initially there were few legal limits on the NSA's ability to conduct electronic surveillance inside the United States. But in the wake of the Church and Pike committee disclosures, Congress passed a law in 1978 that required search warrants, approved by a secret court, for domestic wiretaps in national security cases. That law, the Foreign Intelligence Surveillance Act (FISA), along with other new rules and regulations imposed on the intelligence community in the 1970s and 1980s, effectively ended the NSA's role in domestic surveillance operations.

After those rules were put in place, the FBI, not the NSA, became the primary agency responsible for seeking approval from a special FISA court for national security wiretaps inside the United States. The NSA's domestic role was limited largely to such specialized intelligence activities as the bugging of foreign embassies and diplomatic missions in Washington, New York, and other cities, but even those operations required FISA search warrants.

Hayden wanted the American people to know that the NSA was abiding by the rules.

"Could there be abuses? Of course, there could, but I am looking you and the American people in the eye and saying there are not," Hayden told CNN. "After Church and Pike, on this question, the ball and strike count on the agency is no balls and two strikes," Hayden added. "We don't take any pitches that are close to the strike zone. We are very, very careful. We can't go back to the American people with, 'Oh, well, we're sorry for this one, too.' We don't get close to the Fourth Amendment."

Hayden gave speeches. He went on television, and he talked to

newspaper reporters and to authors writing books about the agency. He even hosted off-the-record dinners for the press at his home at Fort Meade. A key element of Hayden's case was his argument that the NSA was struggling to cope with the rapid pace of change in an age of information overload, a new world of cell phones and BlackBerries and Internet telephone calls. The NSA was collecting more communications than anyone could ever listen to; even its supercomputers, with artificial-intelligence software, had trouble sorting the wheat from the chaff. Downplaying the NSA's capabilities, Hayden liked to say that the NSA was once an information-age organization in the industrial age, and now it was an information-age organization in the information age. It was losing its competitive edge. Commercially available communications technology was catching up. Hayden's implicit message was that the NSA was too archaic, maybe even too incompetent, to spy on America. Hayden didn't say that the NSA was a toothless giant, but he certainly wanted everyone to believe that the NSA was not to be feared.

"Despite what you've seen on television, our agency doesn't do alien autopsies, track the location of your automobile by satellite, nor do we have a squad of assassins," Hayden said reassuringly in a speech at American University in Washington in 2000. "The best I can hope for now is to wipe away some of the mystique surrounding the National Security Agency."

But that was Michael Hayden before 9/11.

Since the attacks, the NSA, with Hayden at the helm until 2005, has been transformed by the Bush administration, in ways that Hayden and other administration officials don't want to talk about. In fact, for the first time since the Watergate-era abuses, the NSA is spying on Americans again, and on a large scale.

The Bush administration has swept aside nearly thirty years of rules and regulations and has secretly brought the NSA back into the

business of domestic espionage. The NSA is now eavesdropping on as many as five hundred people in the United States at any given time and it potentially has access to the phone calls and e-mails of millions more. It does this without court-approved search warrants and with little independent oversight.

President Bush has secretly authorized the NSA to monitor and eavesdrop on large volumes of telephone calls, e-mail messages, and other Internet traffic inside the United States to search for potential evidence of terrorist activity, without search warrants or any new laws that would permit such domestic intelligence collection. Under a secret presidential order signed in early 2002, only months after the September 11 attacks, President Bush has given the NSA the ability to conduct surveillance on communications inside the United States. The secret decision by the president has opened up America's domestic telecommunications network to the NSA in unprecedented and deeply troubling new ways, and represents a radical shift in the accepted policies and practices of the modern U.S. intelligence community.

The NSA is now tapping into the heart of the nation's telephone network through direct access to key telecommunications switches that carry many of America's daily phone calls and e-mail messages. Several government officials who know about the NSA operation have come forward to talk about it because they are deeply troubled by it, and they believe that by keeping silent they would become complicit in it. They strongly believe that the president's secret order is in violation of the Fourth Amendment of the Constitution, which prohibits unreasonable searches, and some of them believe that an investigation should be launched into the way the Bush administration has turned the intelligence community's most powerful tools against the American people.

One government lawyer who is aware of the NSA domestic surveillance operation told reporter Eric Lichtblau that the very few people at the Justice Department who are aware of its existence sim-

ply refer to it as "the Program." It may be the largest domestic spying operation since the 1960s, larger than anything conducted by the FBI or CIA inside the United States since the Vietnam War.

In order to overturn the system established by FISA in 1978, and bring the NSA back into domestic wiretaps without court approval, administration lawyers have issued a series of secret legal opinions, similar to those written in support of the harsh interrogation tactics used on detainees captured in Iraq and Afghanistan. The Bush administration legal opinions that supported the use of harsh interrogation techniques on al Qaeda detainees have, of course, proven controversial, drawing complaints from allies, objections from civil liberties advocates, and court challenges. The administration faced its first serious legal rebuke in June 2004 when the U.S. Supreme Court rejected the administration's effort to hold "enemy combatants" without a hearing. The court warned that "a state of war is not a blank check for the president."

The same could be said about the Program. Yet the NSA domestic spying operation has remained secret, and so the legal opinions and other documents related to the NSA program are still classified.

The administration apparently has several legal opinions to support the NSA operation, written by lawyers at the White House, the CIA, the NSA, and the Justice Department. They all rely heavily on a broad interpretation of Article Two of the Constitution, which grants power to the president as commander in chief of the armed forces. Relying largely on those constitutional powers, Congress passed a resolution just days after the September 11 attacks granting the president the authority to wage a global war on terrorism, and Bush administration lawyers later decided that the war resolution provided the legal basis they needed to support the NSA operation to eavesdrop on American citizens.

While the Bush administration has never publicly discussed the NSA operation, the Justice Department did hint at the administration's thinking on domestic spying in a little-noticed legal brief in an

unrelated court case in 2002. That brief said that "the Constitution vests in the president inherent authority to conduct warrantless intelligence surveillance (electronic or otherwise) of foreign powers or their agents, and Congress cannot by statute extinguish that constitutional authority." The search for foreign "agents" has led the NSA to peer into domestic streams of data.

Debate within the government about the moral and legal issues involved in the NSA operation has been extremely limited because only a handful of high-ranking government officials are aware of the existence of the eavesdropping program. "It was a closed program," said one very senior administration official. "People normally in the chain didn't have access to it."

At the Justice Department, then–Attorney General John Ashcroft was one of the few people informed, and he then brought in a small, select group of like-minded conservative lawyers to help craft some of the legal opinions to buttress the Program. They may have been some of the same lawyers involved in the legal opinions supporting the harsh interrogation techniques.

The NSA eavesdropping operation has been hidden inside a "special access program," a level of secrecy reserved for the government's most sensitive covert operations. "This is the biggest secret I know about," said one official who was deeply troubled by what he knew.

Bush administration officials justify the presidential order by arguing that existing rules curbing the domestic powers of the NSA and CIA impeded the United States in detecting and preventing terrorist attacks. They say that the NSA domestic spying operation is critical to the global war on terrorism, although they offer few specifics. They have not explained why any terrorist would be so naïve as to assume that his electronic communication was impossible to intercept.

* * *

The small handful of experts on national security law within the government who know about the NSA program say they believe it has made a mockery of the public debate over the Patriot Act. The Patriot Act of 2001 has been widely criticized for giving the government too much power to engage in secret searches and to spy on suspects, and even some Republicans chafed at the idea of giving the government still more surveillance powers under an extended and expanded version. The Patriot Act has increased the ability of the nation's intelligence and law-enforcement agencies to monitor conversations and Internet traffic by terrorist suspects with the approval of the special FISA court. But it still requires the FBI to obtain search warrants from the FISA court each time it wants to eavesdrop on a telephone conversation, e-mail message, or other form of communication within the United States. In order to obtain a warrant from the FISA court, the FBI must present evidence to show that the target is linked to a terrorist organization or other foreign agent or power. Even then, the FBI has, in comparison with the NSA, relatively limited technological resources and doesn't have the ability to monitor huge telecommunications networks. It lacks NSA's banks of supercomputers at Fort Meade, believed to be home to the greatest concentration of computing power in the world.

The Patriot Act has given no new powers to the NSA. The Bush administration purposely did not seek congressional approval for the NSA operation, apparently because the White House recognized that it would be too controversial and would almost certainly be rejected. "There is nothing explicit in the Patriot Act for NSA," said one former congressional aide who was involved in the drafting of the Patriot Act, but who was unaware of the NSA operation. "Their surveillance is supposed to be directed outside the United States."

It is now clear that the White House went through the motions of the public debate over the Patriot Act, all the while knowing that the intelligence community was secretly conducting a far more aggres-

sive domestic surveillance campaign. "This goes way beyond the Patriot Act," said one former official familiar with the NSA operation.

President Bush's secret order has given the NSA the freedom to employ extremely powerful computerized search programs—originally intended to scan foreign communications—in order to scrutinize large volumes of American communications. It is difficult to know the precise size of the NSA operation, but one indication of its large scale is the fact that administration officials say that one reason they decided not to seek court-approved search warrants for the NSA operation was that the volume of telephone calls and e-mails being monitored was so big that it would be impossible to get speedy court approval for all of them. It is certainly true that when the FISA court was created, Congress never envisioned that the NSA would be involved in a massive eavesdropping operation inside the United States. No one in the 1970s could have predicted the enormous growth of telecommunications traffic in the United States, or the degree to which Americans would become addicted to digital, electronic communications. Today, industry experts estimate that approximately 9 trillion e-mails are sent in the United States each year. Americans make nearly a billion cell phone calls and well over a billion landline calls each day.

NSA's technical prowess, coupled with its long-standing relationships with the nation's major telecommunications companies, has made it easy for the agency to eavesdrop on large numbers of people in the United States without their knowledge. Following President Bush's order, U.S. intelligence officials secretly arranged with top officials of major telecommunications companies to gain access to large telecommunications switches carrying the bulk of America's phone calls. The NSA also gained access to the vast majority of American e-mail traffic that flows through the U.S. telecommunications system. The identities of the companies involved have been kept secret. Unknown to most Americans, the NSA has extremely close relationships with both the telecommunications and computer industries, ac-

cording to several government officials. Only a very few top executives in each corporation are aware of such relationships or know about the willingness of the corporations to cooperate on intelligence matters.

The main rationale behind the Program, officials said, was that existing rules curbing the domestic powers of the NSA and CIA had left gaps in the ability of the United States to detect and prevent terrorist attacks. They say that one such gap had opened up because many purely international communications—telephone calls and e-mail messages from the Middle East to Asia, for example—end up going through telecommunications switches that are physically based in the United States. As a result, the rules that limit domestic intelligence gathering by the NSA have meant that such international calls could not be monitored, since they were transiting the United States. Some phone calls and e-mail traffic among terrorists operating overseas were being missed by American counterterrorism investigators.

The new presidential order has given the NSA direct access to those U.S.-based telecommunications switches through "back doors." Under the authority of the presidential order, a small group of officials at NSA now monitors telecommunications activity through these domestic switches, searching for terrorism-related intelligence.

To understand how the Bush administration is spying on the American people, it is important to know a few basics about the U.S. telecommunications network. The telephone network today is digital and computerized, but is still built around a switching system that routes calls from city to city, or country to country, as efficiently and quickly as possible.

In addition to handling telephone calls from, say, Los Angeles to New York, the switches also act as gateways into and out of the United States for international telecommunications. A large volume of purely international telephone calls—calls that do not begin or

end in America—also now travel through switches based in the United States. Telephone calls from Asia to Europe, for example, may go through the United States–based switches. This so-called transit traffic has dramatically increased in recent years as the telephone network has become increasingly globalized. Computerized systems determine the most efficient routes for digital "packets" of electronic communications depending on the speed and congestion on the networks, not necessarily on the shortest line between two points. Such random global route selection means that the switches carrying calls from Cleveland to Chicago, for example, may also be carrying calls from Islamabad to Jakarta. In fact, it is now difficult to tell where the domestic telephone system ends and the international network begins.

In the years before 9/11, the NSA apparently recognized that the remarkable growth in transit traffic was becoming a major issue that had never been addressed by FISA or the other 1970s-era rules and regulations governing the U.S. intelligence community. Now that foreign calls were being routed through switches that were physically on American soil, eavesdropping on those calls might be a violation of the regulations and laws restricting the NSA from spying inside the United States.

But transit traffic also presented a major opportunity. If the NSA could gain access to the American switches, it could easily monitor millions of foreign telephone calls, and do so much more consistently and effectively than it could overseas, where it had to rely on spy satellites and listening stations to try to vacuum up telecommunications signals as they bounced through the air. Of course, that would mean NSA would also have direct access to the domestic telephone network as well.

Any debate within the NSA about the legalities of monitoring transit traffic became moot after 9/11. President Bush was determined to sweep away the peacetime rules that had curbed the activities of the U.S. intelligence community since the 1970s, and he readily

agreed to give the NSA broad new powers. The Bush administration's answer has been to place the NSA right into the middle of the American communications bloodstream by giving the agency the secret "trapdoors" into the switching system. One outside expert on communications privacy who previously worked at the NSA said that the United States government has recently been quietly encouraging the telecommunications industry to increase the amount of international communications traffic that is routed through American-based switches. It appears that at least one motive for doing so may be to bring more international calls under NSA scrutiny.

According to government officials, some of the most critical switches are in the New York area, a key intersection between the domestic and international telecommunications networks. Switching facilities in the region feed out to telecommunications cables that dive into the Atlantic Ocean bound for Europe and beyond. The NSA now apparently has access into those switches, allowing it to monitor telecommunications traffic as it enters and exits the United States.

In addition, the NSA has the ability to conduct surveillance on the e-mail of virtually any American it chooses to target. One of the secrets of the Internet is that its infrastructure is dominated by the United States, and that much of the world's e-mail traffic, at one time or another, flows through telecommunications networks that are physically on American soil. E-mail between Germany and Italy, for example, or Pakistan and Yemen, is often routed through America. The secret presidential order has given the NSA the freedom to peruse that international e-mail traffic—along with the e-mail of millions of Americans.

In the Program, the NSA is eavesdropping both on transit traffic—calls from one foreign location to another that are routed through the United States by international telecommunications systems—and on telephone calls and e-mail between people inside the United States and others overseas. Officials who defend the Pro-

gram claim that the NSA tries to minimize the amount of purely domestic telephone and Internet traffic among American citizens that it monitors, to avoid violating the privacy rights of U.S. citizens. But there is virtually no independent oversight of NSA's use of its new power. With its direct access to the U.S. telecommunications system, there seems to be no physical or logistical obstacle to prevent the NSA from eavesdropping on anyone in the United States that it chooses.

NSA also claims that it is eavesdropping only on people suspected of having links to terrorism, but there is no way to confirm exactly who in the United States is being monitored by the agency. According to officials familiar with the NSA operation, it was launched in 2002 after the CIA began to capture high-ranking al Qaeda operatives overseas. At the time of their capture, the CIA also seized their computers, cell phones, and personal phone directories and flew them to the United States for examination.

As the al Qaeda operatives began to fall into American hands, their seized laptops, cell phones, and directories led to the discovery of telephone numbers and e-mail addresses of people with whom they had communicated all around the world. The CIA turned those names, addresses, and numbers over to the NSA, which then began monitoring those numbers, as well as the numbers of anyone in contact with them, and so on outward in an expanding network of phone numbers and Internet addresses, both in the United States and overseas.

In the Program, the NSA determines, on its own, which telephone numbers and e-mail addresses to monitor. The NSA doesn't have to get approval from the White House, the Justice Department, or anyone else in the Bush administration before it begins eavesdropping on a specific phone line inside the United States. Instead, it has set up its own internal checklist to determine whether there is "probable cause" to begin surveillance. The Bush administration argues that the NSA checklist substitutes for the determination of probable

cause in a court of law, but neither federal prosecutors nor other Justice Department attorneys even review the case of a suspect before the NSA begins to listen to his or her phone lines. Occasionally, top Justice Department officials audit the NSA program, but the NSA unilaterally decides on whom to spy. Bush's executive order gives the NSA broad latitude to decide what might constitute a suspicious phone number or e-mail address.

The existence of the Program has been kept so secret that senior Bush administration officials have gone to great lengths to hide the origins of the intelligence it gathers. When the NSA finds potentially useful intelligence in the U.S.-based telecommunications switches, it is "laundered" before it is widely distributed to case officers at the CIA or special agents of the FBI, officials said. Reports are said not to identify that the intelligence came from intercepts of U.S.-based telecommunications.

Bush administration officials offer conflicting information about whether intelligence gathered from the warrantless wiretaps is being used in criminal cases inside the United States. One senior administration official insisted that it never has been used in a criminal trial, but other top officials argued that the eavesdropping program has proved valuable in domestic terrorism investigations. Actually, both statements may be true. It appears that the NSA wiretaps are being used to identify suspects in the United States. But because the intelligence based on the warrantless wiretaps would almost certainly not be admissible in an American court, it is possible that the Bush administration is not attempting to take those cases to trial. Several high-profile terrorism-related cases since 9/11 have ended in plea bargains and out-of-court settlements; few have actually gone to trial. One reason for that legal strategy may be that the administration is fearful of getting caught conducting illegal surveillance operations.

The government has a number of ways to cover up the NSA's role in the domestic surveillance of people inside the United States. In

some instances, the government seeks FISA court approval for wiretaps on individuals who have already been secretly subjected to warrantless eavesdropping by the NSA.

The Bush administration justifies that procedure by saying that the government obtains search warrants if it wants to eavesdrop on the purely domestic telephone calls—between two phones inside the United States—of the individuals under surveillance through the NSA program. Since the NSA is supposed to focus on international "transit traffic" and telephone calls and e-mail messages between someone in the United States and someone overseas, government officials say that they seek FISA warrants when they decide to go further to monitor all of the communications of an individual suspect.

But that process of obtaining a search warrant is clearly tainted. The Bush administration is obtaining FISA court approval for wiretaps at least in part on the basis of information gathered from the earlier warrantless eavesdropping. The government is apparently following that practice with increasing frequency; by the estimate of two lawyers, some 10 percent to 20 percent of the search warrants issued by the secret FISA court now grow out of information generated by the NSA's domestic surveillance program.

Bush administration officials say that the NSA is using the Program to conduct surveillance on the telephone and e-mail communications of about seven thousand people overseas. They also acknowledge that the NSA is targeting the communications of about five hundred people inside the United States. Each one of those individuals is likely to make several phone calls and send several e-mails each day, which could mean that the NSA is eavesdropping on thousands of telephone calls, e-mail messages, and other communications inside the United States on a daily basis. Over time, the NSA has certainly eavesdropped on millions of telephone calls and e-mail messages on American soil.

The expansion of NSA's role from spying on foreigners to conducting domestic surveillance has implications that are sure to pro-

voke objections from civil liberties advocates. Even some senior officials within the administration have raised questions about the Program's legality. Government officials who were aware of the surveillance program "just assumed that something illegal was going on," said one Justice Department official. "People just looked the other way because they didn't want to know what was going on."

Some senior Bush administration officials learned the outlines of the NSA operation but were never officially briefed and were stunned that the White House and Justice Department would approve the domestic spying. "This is really a sea change," said a former senior law enforcement official who questioned both its legal and public-policy aspects. "It's almost a mainstay of this country that the NSA only does foreign searches."

After President Bush signed the secret order authorizing the NSA eavesdropping operation, the Bush administration quietly notified the chief judge on the secret FISA court that approves national security wiretaps. That judge was then–U.S. District Court Judge Royce C. Lamberth, a genial, rotund Texan and a Republican. The administration didn't ask for his approval, and he didn't stand in the way when the government decided not to seek search warrants for the NSA program.

The NSA operation was scaled back, at least briefly, in the spring of 2004 when the federal judge who succeeded Lamberth as chief of the FISA court raised questions about how the NSA program was being used to generate intelligence. The concerns raised by District Court Judge Colleen Kollar-Kotelly clearly rattled the Bush administration. One official said he believed that the Program was effectively halted for about three weeks. Other top administration officials suggested that they abandoned some of the most aggressive techniques used in the NSA surveillance operation after the judge complained.

Some congressional leaders have been notified about the Program, but only in extraordinarily secret fashion and only in ways that

guarantee they feel constrained from raising objections to it. Even when one lawmaker did secretly raise concerns, he was ignored by the White House. In 2002, soon after the NSA operation began, top congressional leaders from both political parties were brought to Vice President Dick Cheney's White House office and were briefed about it by Cheney, Hayden, and then–CIA director George Tenet. The congressional leaders, including Democratic Senator Bob Graham of Florida and Republican Senator Richard Shelby of Alabama, at the time the chairman and vice chairman of the Senate Select Committee on Intelligence, respectively, were not permitted to bring staff members to the meeting and were told not to discuss the matter with anyone else. It was difficult for the congressional leaders to ask any questions about the Program, because they were unable to ask their staff to do any research or oversight of the NSA operation. The congressional leaders apparently knew only what Cheney and other top administration officials told them about the Program.

Later, after new lawmakers took over the intelligence committees, only one congressional leader, Senator Jay Rockefeller, a Democrat of West Virginia, raised any concerns with the White House. After he was first briefed on the matter in early 2003, Senator Rockefeller wrote a letter to Cheney saying that he was troubled by the NSA operation and its potential for the abuse of the civil liberties of American citizens.

Rockefeller told the White House in advance that he was planning to write the letter raising objections. In response, he was told by administration officials that he had to write the letter himself. Rockefeller followed the directions and handed over the letter, but there is no evidence that he ever received a response from Cheney.

The few other Democrats who have been briefed on the operation have fallen into line with the White House, perhaps intimidated by the broad public support for tough counterterrorism measures following 9/11. But at least one other senior Democrat who was briefed later regretted accepting the administration's decision to

launch the operation and realized that the White House had trapped the congressional leaders. By giving the lawmakers secret briefings with no staff present and then demanding that they never discuss the matter with anyone, the congressional leaders were paralyzed. As time wore on, it became increasingly difficult for Democrats to protest the operation, since the White House could argue that they had been receiving briefings for years and had barely complained.

One government lawyer said he went to a congressional official in 2004 to reveal what he knew about the NSA eavesdropping operation because he believed that it was unconstitutional. But nothing happened as a result of his congressional contacts. He did not know that congressional leaders had already been notified.

Apart from the very small number of senior senators and congressmen who have been briefed by the White House on the NSA program, most members of Congress believe that FISA ended, once and for all, the right of the government to conduct secret wiretaps inside the United States without search warrants or court approval. Some experts in national security law say that past presidents have periodically—and very quietly—asserted that despite FISA, they reserved the right to order warrantless wiretaps in the United States under extreme circumstances for national security purposes. But that never became an issue with Congress in the past, because until now, no president has ever actually exercised that authority since FISA became law.

The legal opinions supporting the NSA operation followed secret deliberations over expanding the NSA's role. For example, just days after the September 11, 2001 attacks, John Yoo, a Justice Department lawyer in the Office of Legal Counsel, wrote an internal memorandum that argued that the government might use "electronic surveillance techniques and equipment that are more powerful and sophisticated than those available to law enforcement agencies in order to intercept telephonic communications and observe the movement of persons but without obtaining warrants for such uses." Yoo

noted that while such actions could raise constitutional issues, in the face of devastating terrorist attacks, he wrote, "the government may be justified in taking measures which in less troubled conditions could be seen as infringements of individual liberties."

But that was not an argument that the Bush administration wanted to test openly in Congress. Seeking congressional approval was viewed as politically risky because the proposal would be certain to face intense opposition from civil liberties groups. In order to support the White House decision not to seek new legislation to support the NSA operation, administration lawyers secretly argued that new laws were unnecessary because the post-9/11 congressional resolution on the war on terror provided ample authorization.

In the end, the administration's justifications for the NSA domestic surveillance operation fail to explain adequately why it would not be possible to conduct surveillance of terrorist suspects with court-approved search warrants under the FISA rules. Several government officials said they have not had any trouble obtaining search warrants for wiretaps from the FISA court since the September 11 attacks. The number of warrants approved by the court doubled between 2001 and 2003, when more than 1,700 foreign intelligence warrants were executed, according to the Justice Department. The government has also not had any difficulty in keeping those court-approved wiretaps secret. In the most sensitive cases, the wiretap requests can be handled under such tight security that knowledge of them is restricted to the highest levels of the executive branch on a need-to-know basis.

During the public debate over the Patriot Act, Bush administration officials noted reassuringly that the legislation would not expand the powers of the NSA, as if to underscore their argument that privacy concerns over the Patriot Act were being exaggerated by critics of the legislation. Even Yoo made the point, in an op-ed piece in the *Wall Street Journal,* that the Patriot Act's critics had a cartoonish view

of the law. "Civil libertarians would have us believe that the Patriot Act allows CIA and NSA agents to roam freely through the country detaining anyone they please," Yoo wrote. "Nothing could be further from the truth."

One of the most worrisome aspects of the NSA's move into domestic surveillance is that it appears to be part of a broader series of policies and procedures put in place by the Bush administration that threaten to erode civil liberties in the United States. Across the administration, many questionable actions taken in the heat of the moment after the September 11 attacks have quietly become more permanent, lowering the bar on what is acceptable when it comes to the government's ability to intrude into the personal lives of average Americans. For example, in 2002 the U.S. military expanded its role inside the country with the creation of the new Northern Command, the first military command in recent history that is designed to protect the U.S. homeland. The creation of Northern Command has already raised the specter of military intelligence agents operating on U.S. soil, permanently developing new links with local law enforcement agencies, particularly those near large military bases. Few objections have been raised.

Since the Program was instituted, Hayden has been rewarded by President Bush. In 2005, Hayden was named deputy director of national intelligence, making him the top lieutenant to John Negroponte, the director of national intelligence, the top intelligence post created by the post-9/11 intelligence reforms. During his Senate confirmation hearings for his new position, Hayden was never asked publicly about the NSA's covert domestic intelligence program.

In private, he has been defensive about his role in domestic spy-

ing. Hayden has said that the operations being conducted by NSA are "legal, appropriate, and effective" as part of the war on terrorism. He has little else to say, other than that the matter is "intensely operational." The Program was still active in late 2005, several officials said.