

1 PILLSBURY WINTHROP SHAW PITTMAN LLP
 BRUCE A. ERICSON #76342
 2 DAVID L. ANDERSON #149604
 JACOB R. SORENSEN #209134
 3 BRIAN J. WONG #226940
 50 Fremont Street
 4 Post Office Box 7880
 San Francisco, CA 94120-7880
 5 Telephone: (415) 983-1000
 Facsimile: (415) 983-1200
 6 Email: bruce.ericson@pillsburylaw.com

7 SIDLEY AUSTIN LLP
 DAVID W. CARPENTER (admitted *pro hac vice*)
 8 DAVID L. LAWSON (admitted *pro hac vice*)
 BRADFORD A. BERENSON (admitted *pro hac vice*)
 9 EDWARD R. McNICHOLAS (admitted *pro hac vice*)
 1501 K Street, N.W.
 10 Washington, D.C. 20005
 Telephone: (202) 736-8010
 11 Facsimile: (202) 736-8711
 Email: bberenson@sidley.com

12 Attorneys for Defendants
 13 AT&T CORP. and AT&T INC.

14 UNITED STATES DISTRICT COURT
 15 NORTHERN DISTRICT OF CALIFORNIA
 16 SAN FRANCISCO DIVISION

17
 18 TASH HEPTING, GREGORY HICKS,
 CAROLYN JEWEL and ERIK KNUTZEN
 19 on Behalf of Themselves and All Others
 Similarly Situated,

20 Plaintiffs,

21 vs.

22 AT&T CORP., AT&T INC. and DOES 1-20,
 23 inclusive,

24 Defendants.

No. C-06-0672-VRW

**MOTION OF DEFENDANT
 AT&T CORP. TO DISMISS
 PLAINTIFFS' AMENDED
 COMPLAINT; SUPPORTING
 MEMORANDUM**

Date: June 8, 2006
 Time: 2 p.m.
 Courtroom: 6, 17th Floor
 Judge: Hon. Vaughn R. Walker

Filed concurrently:
 1. Request for judicial notice
 2. Proposed order

TABLE OF CONTENTS

1

2 NOTICE OF MOTION AND MOTION TO DISMISS.....vi

3 ISSUES TO BE DECIDED.....vi

4 MEMORANDUM OF POINTS AND AUTHORITIES..... 1

5 I. INTRODUCTION AND SUMMARY OF ARGUMENT..... 1

6 II. SUMMARY OF THE CASE. 2

7 A. Background..... 2

8 B. Standards for deciding this motion.....4

9 III. ARGUMENT.4

10 A. THE FAC FAILS TO PLEAD THE ABSENCE OF IMMUNITY

11 FROM SUIT.....4

12 1. The FAC fails to plead the absence of absolute statutory

13 immunity.....5

14 a. Numerous statutes provide telecommunications

15 carriers absolute immunity for assisting governmental

16 activities.....5

17 b. Plaintiffs have the burden of pleading facts sufficient

18 to avoid these immunities. 7

19 c. Plaintiffs fail to meet their pleading burden and are

20 relying on extreme and erroneous legal theories..... 10

21 2. The FAC fails to plead the absence of absolute common-law

22 immunity..... 13

23 3. The FAC establishes AT&T’s qualified immunity as a matter

24 of law. 15

25 B. PLAINTIFFS LACK STANDING..... 19

26 1. Plaintiffs have not sufficiently alleged injury-in-fact.....20

27 2. Plaintiffs’ dissatisfaction with government policy does not

28 give them standing..... 22

3. Plaintiffs fail to allege concrete injuries to their statutory

interests..... 24

IV. CONCLUSION.255

1 **TABLE OF AUTHORITIES**

2 **CASES**

3 *Allen v. Wright*,
4 468 U.S. 737 (1984) 19, 23

5 *Baker v. Carr*,
6 369 U.S. 186 (1962) 24

7 *Balistreri v. Pacifica Police Department*,
8 901 F.2d 696 (9th Cir. 1990) 4

9 *Berry v. Funk*,
10 146 F.3d 1003 (D.C. Cir. 1998)..... 16

11 *Blake v. Wright*,
12 179 F.3d 1003 (6th Cir. 1999) 16

13 *Cahill v. Liberty Mutual Insurance Co.*,
14 80 F.3d 336 (9th Cir. 1996) 4

15 *Calloway v. Boro of Glassboro*,
16 89 F. Supp. 2d 543 (D.N.J. 2000)..... 17

17 *City of Los Angeles v. Lyons*,
18 461 U.S. 95 (1983) 23

19 *Clegg v. Cult Awareness Network*,
20 18 F.3d 752 (9th Cir. 1994) 4

21 *Collins v. Jordan*,
22 110 F.3d 1363 (9th Cir. 1996) 18

23 *Conley v. Gibson*,
24 355 U.S. 41 (1957) 4

25 *Craska v. New York Telegraph Co.*,
26 239 F. Supp. 932 (N.D.N.Y. 1965) 14

27 *Crawford-El v. Britton*,
28 523 U.S. 574 (1998) 10, 11

Donohoe v. Duling,
465 F.2d 196 (4th Cir. 1972) 22

Electronic Privacy Information Center, et al. v. Department of Justice,
Civil Action No. 06-00096 (HHK) 1

Flast v. Cohen,
392 U.S. 83 (1968) 20

Fowler v. Southern Bell Telegraph & Telegraph Co.,
343 F.2d 150 (5th Cir. 1965) 14

1	<i>Halkin v. Helms</i> ,	21
	690 F.2d 977 (D.C. Cir. 1982).....	
2		
3	<i>Halperin v. Kissinger</i> ,	14, 15
	424 F. Supp. 838 (D.D.C. 1976),	
	<i>rev'd on other grounds</i> , 606 F.2d 1192 (D.C. Cir.1979).....	
4		
5	<i>Harlow v. Fitzgerald</i> ,	16
	457 U.S. 800 (1982)	
6	<i>Hodgers-Durgin v. de la Vina</i> ,	19
	199 F.3d 1037 (9th Cir. 1999).....	
7		
8	<i>Hunter v. Bryant</i> ,	16
	502 U.S. 224 (1991)	
9	<i>In re Sealed Case</i> ,	12, 18
	310 F.3d 717 (FISA Ct. Rev. 2002)	
10		
11	<i>In re VeriFone Sec. Litigation</i> ,	4
	11 F.3d 865 (9th Cir. 1993).....	
12	<i>In re World War II Era Japanese Forced Labor Litigation</i> ,	23, 24
	164 F. Supp. 2d 1160 (N.D. Cal. 2001).....	
13		
14	<i>Jacobson v. Rose</i> ,	12, 20
	592 F.2d 515 (9th Cir. 1978).....	
15	<i>Kokonnen v. Guardian Life Insurance Co. of America</i> ,	4
	511 U.S. 375 (1994)	
16		
17	<i>Laird v. Tatum</i> ,	22, 23
	408 U.S. 1 (1972)	
18	<i>Lujan v. Defenders of Wildlife</i> ,	19, 21, 23
	504 U.S. 555 (1992)	
19		
20	<i>Mejia v. City of New York</i> ,	17
	119 F. Supp. 2d 232 (E.D.N.Y. 2000).....	
21	<i>O'Shea v. Littleton</i> ,	19, 23, 24
	414 U.S. 488 (1974)	
22		
23	<i>Raines v. Byrd</i> ,	19
	521 U.S. 811 (1997)	
24	<i>Richardson v. McKnight</i> ,	16, 17
	521 U.S. 399 (1997)	
25		
26	<i>Rush v. FDIC</i> ,	16
	747 F. Supp. 575 (N.D. Cal. 1990).....	
27	<i>Schlesinger v. Reservists Committee to Stop the War</i> ,	23
	418 U.S. 208 (1974)	
28		

1	<i>Siegert v. Gilley</i> ,	11
	500 U.S. 226 (1991)	
2		
3	<i>Smith v. Nixon</i> ,	13
	606 F.2d 1183 (D.C. Cir. 1979).....	
4	<i>Sprewell v. Golden State Warriors</i> ,	4
	266 F.3d 979 (9th Cir. 2001)	
5		
6	<i>Tapley v. Collins</i> ,	13, 16
	211 F.3d 1210 (11th Cir. 2000)	
7	<i>Tenet v. Doe</i> ,	9, 10
	544 U.S. 1, 125 S. Ct. 1230 (2004)	
8		
9	<i>Thompson v. Dulaney</i> ,	8
	970 F.2d 741 (10th Cir. 1992)	
10	<i>Totten v. United States</i> ,	9
	92 U.S. 105 (1876)	
11		
12	<i>United Presbyterian Church v. Reagan</i> ,	21, 22
	738 F.2d 1375 (D.C. Cir. 1984).....	
13	<i>United States v. Goldstein</i> ,	9
	532 F.2d 1305 (9th Cir. 1976)	
14		
15	<i>United States v. Reynolds</i> ,	9
	345 U.S. 1 (1953)	
16	<i>United States v. SCRAP</i> ,	24
	412 U.S. 669 (1973)	
17		
18	<i>United States v. Texas</i> ,	13
	507 U.S. 529 (1993)	
19	<i>United States v. United States Dist. Court (Keith)</i> ,	18
	407 U.S. 297 (1972)	
20		
21	<i>Valley Forge Christian College v. Americans United for Separation of Church and</i>	
	<i>State, Inc.</i> ,	
22	454 U.S. 464 (1982)	19, 20, 23
23	<i>Vernon v. City of Los Angeles</i> ,	22
	27 F.3d 1385 (9th Cir. 1994).....	
24	<i>Warren v. Fox Family Worldwide, Inc.</i> ,	4, 11
	328 F.3d 1136 (9th Cir. 2003)	
25		
26	<i>Warth v. Seldin</i> ,	19
	422 U.S. 490 (1975)	
27	<i>White v. Lee</i> ,	4
	227 F.3d 1214 (9th Cir. 2000)	
28		

1 *Williams v. Poulos*,
 11 F.3d 271 (1st Cir. 1993) 7, 8

2
 3
 4
 5
 6
 7
 8
 9
 10
 11
 12
 13
 14
 15
 16
 17
 18
 19
 20
 21
 22
 23
 24
 25
 26
 27
 28

STATUTES AND OTHER AUTHORITY

18 U.S.C. § 798(a)(3) 10

18 U.S.C. § 2511 passim

18 U.S.C. § 2520 7, 8, 12

18 U.S.C. § 2702 6, 9

18 U.S.C. § 2703 5, 6, 9, 10, 12

18 U.S.C. § 3124(d)..... 6

47 U.S.C. § 605 6, 8, 9

50 U.S.C. § 1801 24

50 U.S.C. § 1805(i)..... 6

50 U.S.C. § 1809 24

50 U.S.C. § 1810 24

Cal. Bus. & Prof. Code §17200..... 25

Cal. Bus. & Prof. Code §17204..... 25

Federal Rule of Civil Procedure Rule 12(b)(1) vi, 4

Federal Rule of Civil Procedure Rule 12(b)(6) vi, 4

Senate Report No. 99-541 (1986)..... 8

Senate Report No. 95-604 (1978)..... 12

Terrorist Surveillance Act of 2006, S. 2455, 109th Cong., 2d Sess. 24

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

NOTICE OF MOTION AND MOTION TO DISMISS

TO ALL PARTIES AND THEIR COUNSEL OF RECORD:

PLEASE TAKE NOTICE that on Thursday, June 8, 2006, at 2:00 p.m., before the Honorable Vaughn R. Walker, United States District Chief Judge, in Courtroom 6, 17th Floor, 450 Golden Gate Avenue, San Francisco, California, defendant **AT&T CORP.** (“AT&T”) will move and hereby does move, pursuant to Rules 12(b)(1) and 12(b)(6) of the Federal Rules of Civil Procedure, to dismiss the Amended Complaint for Damages, Declaratory and Injunctive Relief (Dkt. 8, referred to hereafter as the “Amended Complaint” or the “FAC”) filed by plaintiffs Tash Hepting, Gregory Hicks, Carolyn Jewel and Erik Knutzen (collectively, “plaintiffs”) on February 22, 2006.

This motion is made on the grounds that plaintiffs have failed to meet their burden to plead that defendants lack statutory and common law immunity from suit and that plaintiffs do not have standing to pursue this lawsuit.

This motion is based on this notice of motion and motion, the memorandum that follows, the request for judicial notice filed herewith, the administrative motion filed herewith, all pleadings and records on file in this action, and any other arguments and evidence presented to this Court at or before the hearing on this motion.

ISSUES TO BE DECIDED

1. On the facts as alleged by the plaintiffs, have plaintiffs met their burden to negate the statutory and common law immunities applicable to telecommunications providers that are requested and authorized by the government to lend assistance to government surveillance activities?

2. Do the named plaintiffs have standing to challenge alleged government surveillance activities if their complaint does not allege facts—as opposed to unsupported belief—suggesting that they have been or will be the targets of such surveillance?

1 **MEMORANDUM OF POINTS AND AUTHORITIES**

2 **I. INTRODUCTION AND SUMMARY OF ARGUMENT.**

3 This lawsuit arises out of a disagreement with the federal government’s national
4 security policies. Through this lawsuit, the Plaintiffs seek to challenge intelligence
5 activities allegedly carried out by the National Security Agency (“NSA”) at the direction of
6 the President, as part of the government’s effort to prevent terrorist attacks by al Qaeda and
7 other associated groups. Plaintiffs believe these activities to be unlawful, allege that AT&T
8 is assisting the NSA with those activities, and seek through this lawsuit to hold AT&T
9 liable for its alleged assistance. Whatever the truth of plaintiffs’ allegations or the merits of
10 the underlying dispute over the lawfulness of the NSA surveillance activities acknowledged
11 by the President (hereinafter “the Terrorist Surveillance Program” or “Program”), this case
12 has been brought by the wrong plaintiffs and it names the wrong defendants. The real
13 dispute is between any actual targets of the Program and the government.¹ It cannot
14 involve telecommunications carriers (such as AT&T) who are alleged only to have acted in
15 accord with requests for assistance from the highest levels of the government in sensitive
16 matters of national security. And the dispute does not involve average AT&T customers
17 (such as plaintiffs) with no perceptible connection to al Qaeda or international terrorism.

18 Yet rather than seeking to vindicate their position through the political process,
19 plaintiffs have sued AT&T for allegedly providing the government with access to its
20 facilities, even though they do not allege that AT&T acted independently or for any reasons

21
22 ¹ There are numerous other cases pending around the country that challenge the Program
23 directly, either through complaints filed by public interest groups or in the context of
24 criminal cases or asset-blocking actions in which terrorism suspects have suffered
25 concrete adverse consequences due to governmental enforcement actions. *See, e.g.,*
26 *American Civil Liberties Union et al. v. NSA et al.*, Civ. 06-10204 (E.D. Mich.); *Center*
27 *for Constitutional Rights v. Bush et al.*, Civ. 06-313 (S.D.N.Y.); *Electronic Privacy*
28 *Information Center, et al. v. Department of Justice*, Civ. No. 06-00096 (HHK) (D.D.C.);
Al-Haramain Islamic Foundation, Inc., et al. v. George W. Bush, et al., CV-06-274-MO
(D. Ore.); *United States v. al-Timimi*, No. 1:04cr385 (E.D. Va.); *United States v. Aref*,
Crim. No. 04-CR-402 (N.D.N.Y.); *United States v. Albanna, et al.*, Crim. No. 02-CR-
255-S (W.D.N.Y.); *United States v. Hayat, et al.*, Crim. No. S-05-240-GEB (E.D. Cal.).
Copies of select related complaints and other filings are attached to defendants’ request
for judicial notice, filed herewith (“RFJN”) as Exs. A through I.

1 of its own. On the contrary, plaintiffs allege that AT&T acted at all times at the direction
2 and with the approval of the United States government. *See, e.g.*, FAC ¶ 82. If these
3 allegations were true, it is the government and not AT&T that would be obliged to answer
4 for the lawfulness of the challenged intelligence activities: both Congress and the courts
5 have conferred blanket immunity from suit on providers of communications services who
6 respond to apparently lawful requests for national security assistance from the federal
7 government. We are aware of no case in which a telecommunications carrier – even when
8 known to be involved in such activities – has ever been held liable for allowing or assisting
9 government-directed surveillance. As a result, whether or not it had any role in the
10 Program, AT&T is entitled to immediate dismissal.

11 Moreover, Plaintiffs do not allege any fact suggesting that they themselves have
12 suffered any known, concrete harm from the Terrorist Surveillance Program. Indeed, their
13 allegations expressly place them *outside* the category of targets of the Program, making the
14 likelihood that they have suffered any sort of injury from the Program even lower than the
15 likelihood that would apply to any other American who occasionally makes international
16 calls or surfs the Internet. They thus lack Article III standing. Their disagreement with the
17 government’s surveillance activities may be passionate and sincerely felt, but a passionate
18 and sincere disagreement with governmental policy is not enough to confer standing.

19 **II. SUMMARY OF THE CASE.**

20 **A. Background.**

21 Plaintiffs allege that AT&T provides the NSA with access to its telecommunications
22 facilities and databases as part of an electronic surveillance program authorized directly by
23 the President. *See* FAC ¶¶ 3-6.² Plaintiffs claim that “at all relevant times, the government
24 instigated, directed and/or tacitly approved all of the . . . acts of AT&T Corp.” *Id.* ¶ 82.
25 Plaintiffs do not allege that AT&T carried out any actual electronic surveillance; rather, the

26
27 ² As it must, AT&T accepts plaintiffs’ allegations as true solely for purposes of this
28 motion, and nothing herein should be construed as confirmation by AT&T of any
involvement in the Program or other classified activities.

1 gravamen of the complaint is that AT&T allegedly provided access to databases and
2 telecommunications facilities that enabled the government to do so. *Id.* ¶ 6 (“AT&T Corp.
3 has opened its key telecommunications facilities and databases to direct access by the NSA
4 and/or other government agencies . . .”); *see also id.* ¶¶ 38, 41-42, 46, 51, 61.

5 Plaintiffs base their allegations on newspaper reports of the classified Terrorist
6 Surveillance Program that the President has stated he authorized after September 11, 2001
7 and later reauthorized more than 30 times. FAC ¶¶ 3, 32-33. But plaintiffs’ reading of the
8 newspapers is selective. They refer to public statements of the President and the Attorney
9 General, *see id.* ¶¶ 33-35, but they omit the Attorney General’s description of two key
10 characteristics of the Terrorist Surveillance Program: first, it intercepts the contents of
11 communications where “one party to the communication is outside the United States”—in
12 other words, international communications; second, it intercepts the contents of
13 communications only if the government has “a reasonable basis to conclude that one party
14 to the communication is a member of al Qaeda, affiliated with al Qaeda, or a member of an
15 organization affiliated with al Qaeda, or working in support of al Qaeda.”³

16 Plaintiffs purport to bring this case on behalf of a massive, nationwide class of all
17 individuals who are or were subscribers to AT&T’s services at any time after September
18 2001, and a subclass of California residents. FAC ¶¶ 65-68. But their putative classes
19 expressly exclude the targets of the program described by the Attorney General—any
20 “foreign powers . . . or agents of foreign powers . . . , including without limitation anyone
21 who knowingly engages in sabotage or international terrorism, or activities in preparation
22 therefore.” *Id.* ¶ 70 (citations omitted). Plaintiffs do not allege that they themselves
23 communicate with anyone who might be affiliated with al Qaeda.

24

25

26 ³ Press Briefing by Attorney General Alberto Gonzales and General Michael Hayden,
27 Principal Deputy Director for National Intelligence, *available at* <http://www.whitehouse.gov/news/releases/2005/12/20051219-1.html> (Dec. 19, 2005) (statement of Attorney
28 General Gonzales), attached as RFJN Ex. J and also as Attachment 2 to Plaintiff’s request
for judicial notice (Dkt. 20).

1 **B. Standards for deciding this motion.**

2 This motion is made under Rule 12(b)(1) and Rule 12(b)(6). Under Rule 12(b)(6), a
3 case is properly dismissed when the plaintiff can prove no set of facts that would entitle him
4 or her to relief. *Conley v. Gibson*, 355 U.S. 41, 45-46, 78 S. Ct. 99 (1957); *Cahill v. Liberty*
5 *Mut. Ins. Co.*, 80 F.3d 336, 338 (9th Cir. 1996). The court must consider whether,
6 assuming the truth of the complaint’s factual allegations, the plaintiff has stated a claim for
7 relief. Dismissal can be based “on the lack of a cognizable legal theory or the absence of
8 sufficient facts alleged under a cognizable legal theory.” *Balistreri v. Pacifica Police*
9 *Dep’t*, 901 F.2d 696, 699 (9th Cir. 1990). Only allegations of fact are taken as true under
10 Rule 12(b)(6). “Conclusory allegations of law and unwarranted inferences are insufficient
11 to defeat a motion to dismiss for failure to state a claim.” *In re VeriFone Sec. Litig.*,
12 11 F.3d 865, 868 (9th Cir. 1993); *Clegg v. Cult Awareness Network*, 18 F.3d 752, 754-55
13 (9th Cir. 1994); *Sprewell v. Golden State Warriors*, 266 F.3d 979, 988 (9th Cir. 2001).

14 Under Rule 12(b)(1), it is presumed that the court lacks jurisdiction, and the plaintiff
15 bears the burden of establishing subject matter jurisdiction. *Kokonnen v. Guardian Life Ins.*
16 *Co.*, 511 U.S. 375, 377, 114 S. Ct. 1673 (1994). Absent jurisdiction, the court must dismiss
17 the case. When a Rule 12(b)(1) motion attacks the court’s jurisdiction as a matter of fact,
18 the court is not limited to the allegations of the complaint and may consider extrinsic
19 evidence, including matters of public record. *Warren v. Fox Family Worldwide, Inc.*,
20 328 F.3d 1136, 1139 (9th Cir. 2003); *White v. Lee*, 227 F.3d 1214, 1242 (9th Cir. 2000).

21 **III. ARGUMENT.**

22 **A. THE FAC FAILS TO PLEAD THE ABSENCE OF IMMUNITY FROM SUIT.**

23 Both Congress and the courts have recognized an overriding policy interest in
24 having telecommunications carriers cooperate with government requests for national
25 security or foreign intelligence assistance, leaving the defense of substantive challenges to
26 such activity to the government or the political process. For this reason, carriers who
27 respond to apparently lawful requests for assistance from the federal government enjoy
28 statutory and common-law immunity from suit. The FAC does not allege that AT&T

1 engaged in any surveillance of its own or for its own reasons, or undertook any action
2 without the direction or approval of the federal government; in fact, it affirmatively alleges
3 the opposite. *See* FAC ¶¶ 82-84. Thus, even assuming *arguendo* the truth of plaintiffs'
4 allegations, plaintiffs have failed to negate the statutory and common-law immunities that
5 protect carriers such as AT&T from suit, and AT&T is entitled to immediate dismissal.
6 Plaintiffs ultimately rest their complaint on an extreme legal theory that is simply wrong.

7 **1. The FAC fails to plead the absence of absolute statutory immunity.**

8 **a. Numerous statutes provide telecommunications carriers absolute**
9 **immunity for assisting governmental activities.**

10 In numerous places in the United States Code, Congress has made clear that where
11 the government authorizes a communications provider to cooperate with governmental
12 surveillance, that provider is immune from suit. The FAC alleges only that AT&T acted as
13 an agent of, and at the direction of, the government, and that the Program was authorized
14 and repeatedly reauthorized by the President. FAC ¶¶ 3-6, 82-85. Thus, whatever one's
15 views of the Program, assuming for the sake of argument that the allegations of the FAC
16 were true, it could not be challenged by suing AT&T.

17 Both 18 U.S.C. § 2511(2)(a)(ii) and 18 U.S.C. § 2703(e) provide absolute immunity
18 from any and all claims arising out of the surveillance activities alleged in the FAC:

19 *Notwithstanding any other law, providers of wire or*
20 *electronic communication service, their officers, employees*
21 *and agents . . . are authorized to provide information,*
22 *facilities, or technical assistance to persons authorized by law*
23 *to intercept wire, oral, or electronic communications or to*
conduct electronic surveillance as defined in section 101 of
[FISA]. . . if such provider, its officers, employees, or
agents, . . . has been provided with –

24 (B) a certification in writing by a person specified in
25 section 2518 (7) of this title or the Attorney General of the
26 United States that no warrant or court order is required by
27 law, that all statutory requirements have been met, and that
28 the specified assistance is required

1 18 U.S.C. § 2511(2)(a)(ii) (emphasis added). Immunity under this provision is absolute:
2 “No cause of action shall lie in any court against any provider of wire or electronic
3 communication service, its officer, employees, or agents, . . . for providing information,
4 facilities, or assistance in accordance with the terms of a . . . certification under this
5 chapter.” *Id.* (emphasis supplied).

6 In like fashion, the ECPA confers absolute immunity on communication providers
7 acting with government authorization:

8 *No cause of action shall lie in any court against any provider*
9 *of wire and electronic communication service, its officers,*
10 *employees, agents, or other specified persons providing*
11 *information, facilities, or assistance in accordance with the*
12 *terms of a . . . statutory authorization, or certification under*
13 *this chapter.*

14 18 U.S.C. § 2703(e) (emphasis added).⁴

15 Together, these provisions confer absolute immunity on communications carriers
16 authorized to assist the government in foreign intelligence surveillance. This immunity
17 ensures that intelligence matters will not be aired in the nation’s courts and eliminates the
18 risk that courts of general jurisdiction will issue orders that might impede the government’s
19 ability to obtain intelligence that may be critical to protecting the country against foreign
20 attack. This immunity also ensures that the government can obtain prompt cooperation
21 from communications providers in meeting national security needs, without the chilling
22 effect of potential civil liability. Providers will almost always lack the factual information
23 necessary to evaluate the necessity or propriety of classified intelligence activities; to assure
24 that they do not have to argue or equivocate when the government asks for help, the risk of

24 ⁴ “[T]his chapter” includes 18 U.S.C. § 2702(b)(2) , which cross references 18 U.S.C.
25 § 2511(2)(a)(ii), making clear that the immunity extends to certifications for foreign
26 intelligence surveillance under the latter provision. FISA and the Communications Act
27 both contain analogous immunity provisions. *See* 50 U.S.C. § 1805(i) (immunity for
28 providing assistance “in accordance with a court order or request for emergency
assistance under this chapter”); 47 U.S.C. § 605(a)(6) (immunity for providing
investigative assistance “on demand of other lawful authority”); *see also* 18 U.S.C.
§ 3124(d) (immunity for compliance with pen register requests).

1 liability for wrongful foreign intelligence surveillance activities is placed not on the
2 providers but on the government.

3 **b. Plaintiffs have the burden of pleading facts sufficient to avoid**
4 **these immunities.**

5 Congress gave plaintiffs the burden to plead specific facts demonstrating the
6 absence of immunity when suing a communications provider for allegedly assisting the
7 government with surveillance. By providing that “no cause of action shall lie” against
8 providers who have acted in accord with governmental authorizations, Congress made the
9 absence of immunity an element of plaintiffs’ claims – and not an affirmative defense.

10 That is reflected in the provisions of the Act that provide for causes of action. For
11 example, the FAC’s Count III alleges interception and disclosure of communications in
12 violation of 18 U.S.C. § 2511 under a right of action created by 18 U.S.C. § 2520(a). In
13 defining that right of action, Congress provided that:

14 *Except as provided in section 2511(2)(a)(ii), any person*
15 *whose wire, oral, or electronic communication is intercepted,*
16 *disclosed or intentionally used in violation of this chapter*
17 *may in a civil action recover from the person or entity, other*
than the United States, which engaged in that violation such
relief as may be appropriate.

18 *Id.* (emphasis added). The highlighted language makes clear that, to state a claim for a
19 violation of § 2520(a), a plaintiff must allege facts showing that the immunities of
20 § 2511(2)(a)(ii) do not apply. None of the other statutory exceptions to § 2511—*e.g.*, the
21 switchboard-operator exception (§ 2511(2)(a)(i)), the FCC exception (§ 2511(2)(b)), or the
22 consent exception (§ 2511(2)(c))—is similarly referenced in § 2520’s definition of the
23 cause of action. Only the absence of an immunity under § 2511(2)(a)(ii) was singled out by
24 Congress as a necessary element of any claim under § 2520.⁵ *Cf. Williams v. Poulos,*

25

26 ⁵ 18 U.S.C. § 2520(d) further provides that it “is a complete defense against any civil or
27 criminal action brought under this chapter or *any other law*” (emphasis added) that the
28 provider acted in “good faith reliance” on “a statutory authorization” or based on a “good
faith determination” that the required authorization under § 2511(2)(a)(ii) existed. The
(continued...)

1 11 F.3d 271, 284 (1st Cir. 1993) (plaintiff’s burden of proof in an action under 18 U.S.C.
2 § 2520 includes demonstrating that § 2511 immunity does not apply); *Thompson v.*
3 *Dulaney*, 970 F.2d 744, 749 (10th Cir. 1992) (same). Because § 2511(2)(a)(ii) immunity
4 precludes liability on any theory in any court, the same rule necessarily applies to all causes
5 of action based on the same alleged conduct.

6 The legislative history of ECPA confirms that Congress intended providers to be
7 relieved of the burdens of litigation when complying with government requests for
8 assistance. With respect to § 2520(a), authorizing civil suits against violators of § 2511,
9 Senate Report No. 99-541 (1986) states:

10 Proposed subsection 2520(a) of title 18 authorizes the
11 commencement of a civil suit. There is one exception. A
12 civil action will not lie where the requirements of section
13 2511(2)(a)(ii) of title 18 are met. With regard to that
exception, the Committee intends that the following
procedural standards will apply:

14 (1) The *complaint must allege* that a wire or electronic
15 communications service provider (or one of its employees):
16 (a) disclosed the existence of a wiretap; (b) acted without a
17 facially valid court order or certification; (c) acted beyond the
18 scope of a court order or certification or (d) acted on bad
faith. . . . *If the complaint fails to make any of these*
allegations, the defendant can move to dismiss the complaint
for failure to state a claim upon which relief can be granted.

19 *Id.* at 26 (reprinted in 1986 U.S.C.C.A.N. 3555, 3580) (emphasis supplied). In addition, the
20 Report explains that “in the absence of [a criminal] prosecution and conviction [for the acts
21 complained of], it is the *plaintiff’s burden* to establish that the requirements of [section
22 2520] are met.” *Id.* at 27. (emphasis supplied). The specifics of other statutes at issue
23 reinforce this understanding.⁶

24 _____
25 (...continued)
26 designation of “good faith reliance” as a “defense” indicates that § 2511(2)(a)(ii)
delineates something that is more than a defense – *i.e.*, an affirmative requirement that
any § 2520(a) claim must allege that § 2511(2)(a)(ii) does not apply.

27 ⁶ For example, 47 U.S.C. § 605 (FAC Count IV) expressly includes the absence of
28 § 2511(2)(a)(ii) immunity as an element of plaintiffs’ claim. *Cf. United States v.*

(continued...)

1 Well-established judicial precedents and principles of national security law
2 reinforce the wisdom and necessity of these congressionally-mandated pleading rules.
3 Courts considering suits involving secret military or intelligence programs have long held
4 that the question of immunity should be decided at the outset. In *Tenet v. Doe*, 544 U.S. 1,
5 125 S. Ct. 1230 (2004), for example, the Supreme Court recently reaffirmed a line of
6 precedent stretching back more than a century barring lawsuits against the government
7 based on secret espionage agreements. This rule was announced in *Totten v. United States*,
8 92 U.S. (2 Otto) 105 (1876), which barred an action by a man who claimed that President
9 Lincoln had hired him at \$200 a month to spy on the “insurrectionary States.” *Totten*,
10 92 U.S. at 105-06. The rule holds that “where success [in litigation] depends upon the
11 existence of [a] secret espionage relationship,” *Tenet*, 125 S. Ct. at 1236, a lawsuit must be
12 “dismissed on the pleadings without ever reaching the question of evidence,” *id.* at 1237
13 (quoting *United States v. Reynolds*, 345 U.S. 1, 11 n.26 (1953) (emphasis omitted)). The
14 *Tenet* Court specifically noted that the “absolute protection” afforded by the *Totten*
15 immunity was “designed not merely to defeat the asserted claims, but to preclude judicial
16 inquiry.” *Tenet*, 125 S. Ct. at 1235 n.4, 1237. As such, national security-related immunity
17 “represents the sort of threshold question we have recognized may be resolved before
18 addressing jurisdiction.” *Id.* at 1235 n.4 (internal quotation marks omitted).

19 The statutory immunities provided to telecommunications carriers in this context
20 are, like the rules of dismissal in *Totten* and *Tenet* – and for like reasons – designed to

21 (…continued)

22 *Goldstein*, 532 F.2d 1305, 1312 (9th Cir. 1976) (“The language of the amendment to
23 § 605 providing that “except as authorized by chapter 119, title 18, United States
24 Code’ no person may disclose certain wire communications, is a clear manifestation
25 of Congress’ intent that § 605 shall not limit § 2511 investigations.”). And 18 U.S.C.
26 § 2702(a)(1), (2), and (3) (FAC Counts V and VI) are subject to the same requirement.
27 Section 2702 states that “[e]xcept as provided in subsection (b),” it is illegal for persons
28 or entities providing either an “electronic communication service” or a “remote
computing service” to make certain disclosures. Subsection (b)(2) makes lawful the
disclosure of the contents of communications “as otherwise authorized in section 2517,
2511(2)(a), or 2703 of this title” (emphasis added). Because the statutory prohibition
itself expressly incorporates and permits any disclosure authorized by § 2511(2)(a), these
statutory causes of action, too, make the absence of § 2511(2)(a)(ii) immunity an element
of the claim and part of plaintiffs’ pleading burden.

1 provide “absolute protection” from such claims. *Id.* at 1236-37. Sections 2711(2)(a)(ii)
2 and 2703(3) both specify that “[n]o cause of action shall lie in any court” if a provider is
3 acting pursuant to governmental authorization. This powerful language assures
4 communications providers that cooperation with the government will not subject them to
5 the burdens of litigation. Where parties are entitled to immunity from suit, “there is a
6 strong public interest in protecting [them] from the costs associated with the defense of
7 damages actions”—an interest best served by dismissing questionable lawsuits
8 expeditiously. *Crawford-El v. Britton*, 523 U.S. 574, 596, 118 S. Ct. 1584 (1998).

9 Immunities such as these are “designed not merely to defeat the asserted claims, but
10 to preclude judicial inquiry.” *Tenet*, 125 S. Ct. at 1235 n.4. That makes particular sense
11 where, as here, if plaintiffs’ allegations were correct, defendants would not be able to
12 mount a factual defense without violating legal prohibitions on disclosure of classified
13 information pertaining to surveillance. *See, e.g.*, 18 U.S.C. § 798(a)(3) (criminalizing
14 disclosure of classified information “concerning the communication intelligence activities
15 of the United States”); 18 U.S.C. § 2511(2)(a)(ii) (forbidding disclosure of “any
16 interception or surveillance” or the “device” used to accomplish it pursuant to government
17 authorized programs). Unless suits making allegations like those in this case (whether true
18 or false) could be dismissed on immunity grounds at the pleading stage, it would be
19 impossible to respect the imperative to “preclude judicial inquiry” into sensitive matters
20 involving the sources and methods of gathering foreign intelligence that Congress and the
21 Executive have concluded must be kept confidential.

22 **c. Plaintiffs fail to meet their pleading burden and are relying on**
23 **extreme and erroneous legal theories.**

24 Plaintiffs fail to meet their burden of alleging specific facts that negate the
25 applicability of statutory immunity. Plaintiffs allege no facts suggesting that, even
26 assuming AT&T engaged in the conduct alleged, AT&T lacked government authorization
27
28

1 under § 2511(2)(a)(ii).⁷ Nor could they: the facts necessary to make (or refute) such an
2 allegation – even assuming they existed – would be completely unavailable to plaintiffs and
3 impossible for either party ever to bring into court.

4 But the flaw in the FAC is even deeper: its allegations, even if true, affirmatively
5 tend to suggest immunity. The gravamen of the FAC is that AT&T allegedly complied
6 with requests to assist in a foreign intelligence program that had been authorized at the
7 highest levels of government. FAC ¶¶ 84-85. Plaintiffs assert that the President himself
8 authorized the Program more than 30 times, *see* FAC ¶ 33, and the Attorney General
9 himself has personally defended it. Most pertinently, plaintiffs expressly allege that “the
10 government instigated, directed and/or tacitly approved all of the . . . acts of AT&T Corp,”
11 FAC ¶ 82, and that “AT&T Corp. acted as an instrument or agent of the government,” *id.*
12 ¶ 85. This, by its terms, is an allegation that AT&T acted in accord with governmental
13 authorization. There is no suggestion in the FAC that, if AT&T acted, it did so on its own,
14 for its own purposes, or outside the governmental authorization plaintiffs allege.

15 Plaintiffs have elsewhere admitted these points. *See* Pl. Mem. in Support of Mot.
16 for Prelim. Inj. at 19-21. In their injunction papers, they acknowledge that the relevant
17 federal statutes preclude suits against carriers when those carriers receive certain
18 governmental authorizations. Yet here, too, plaintiffs do *not* contend that such
19 authorizations were not provided to AT&T in connection with its alleged assistance.
20 Rather, plaintiffs’ arguments assume that governmental authorizations *were* provided to
21 AT&T, and then go on to defend their complaint under an extreme legal theory that is
22 simply wrong.

23

24 ⁷ The conclusory allegation that AT&T’s actions were “without lawful authorization,” FAC
25 ¶ 81, cannot meet this burden. In this setting, “a ‘firm application of the Federal Rules of
26 Civil Procedure’ is fully warranted,” including but not limited to “insist[ing] that the
27 plaintiff ‘put forward specific nonconclusory factual allegations’ . . . in order to survive a
28 precovery motion for dismissal or summary judgment.” *Crawford-El*, 523 U.S. at 598
(*quoting* *Siebert v. Gilley*, 500 U.S. 226, 236 (1991) (Kennedy, J., concurring)). In any
event, FAC ¶ 81 states a legal conclusion that need not be accepted as true on a motion to
dismiss. *Warren*, 328 F.3d at 1139, 1141 n.5.

1 In particular, their legal theory is that, although § 2511(2)(a)(ii) and § 2703(e)
2 categorically provide that “no cause of action lies” against a telecommunications carrier
3 who has acted in accord with governmental authorization, these provisions somehow do not
4 mean what they say. Rather, plaintiffs contend that immunity exists only where
5 authorization has been issued in one of the four circumstances in which FISA specifically
6 authorizes warrantless surveillance and that none of these conditions exists here. This
7 contention is wrong. If Congress had intended to narrow the immunity to those four
8 situations, it would have said so. Congress did not do so because it recognized that where
9 the Attorney General or other responsible officials have authorized surveillance in sensitive
10 areas of national security, it cannot be the province of telecommunications carriers to
11 second-guess them, especially without having the facts to do so.⁸

12 The legal authorities that plaintiffs cite are inapposite. Plaintiffs rely on *Jacobson v.*
13 *Rose*, 592 F.2d 515 (9th Cir. 1978), but that was a case in which the telephone company
14 had *not* acted in accord with a governmental authorization and in which it did not enjoy the
15 absolute immunity of § 2511(2)(a). The Court thus addressed the issue whether the
16 company could rely on the separate good faith immunity conferred by 18 U.S.C. § 2520.
17 Here, by contrast, the issue is absolute statutory immunity, and plaintiffs’ failure to plead its
18 inapplicability cannot be cured by their legal argument that the Program falls outside the
19 four categories of warrantless surveillance authorized by the FISA statute. Even if that
20 were true, it would be a potential legal problem only for the government; it does not affect

21

22 ⁸ To support their attempt to rewrite the immunity provisions of the statutes, plaintiffs refer
23 to the provision of FISA that states that its procedures are the exclusive means of
24 conducting certain surveillance and interceptions. 18 U.S.C. § 2511(f). But this
25 argument ignores that, when FISA was enacted, Congress clearly understood that there
26 were significant areas of warrantless foreign intelligence surveillance the President would
27 continue to direct solely pursuant to his inherent constitutional authority . S. Rep. No. 95-
28 604 at 64 (1978), *reprinted in* 1978 U.S.C.C.A.N. 3904, 3965 ((FISA “does not deal with
international signals intelligence activities as currently engaged in by the National
Security Agency and electronic surveillance conducted outside the United States”). Even
after the passage of FISA, the courts have recognized the President’s continuing
constitutional authority in this area, *See, e.g., In re Sealed Case*, 310 F.3d 717, 742
(FISA Ct. Rev. 2002).

1 the immunity of telecommunications providers under § 2511(2)(a).

2 In short, whatever the merits of the current national debate over the legal authority
3 for the Program, plaintiffs are here alleging only that AT&T acted pursuant to
4 governmental authorization. As such, their allegations are insufficient to permit this lawsuit
5 to go forward in light of the clear statutory immunities enacted by Congress.

6 **2. The FAC fails to plead the absence of absolute common-law immunity.**

7 Not only the Congress but also the courts have long recognized the importance of
8 insulating against suit telecommunications carriers that cooperate with foreign intelligence
9 or law enforcement investigations conducted by the government. The statutory immunities
10 described above were enacted against a backdrop of strong common-law immunities.
11 These common-law immunities too require dismissal of this lawsuit.

12 Statutes in derogation of the common law “are to be read with a presumption
13 favoring the retention of long-established and familiar principles, except when a statutory
14 purpose to the contrary is evident.” *United States v. Texas*, 507 U.S. 529, 534 (1993)
15 (internal quotation marks omitted). The statutory immunities evince no congressional
16 purpose to displace, rather than supplement, the common law. *See, e.g., Tapley v. Collins*,
17 211 F.3d 1210, 1216 (11th Cir. 2000) (“[t]he Federal Wiretap Act lacks the specific,
18 unequivocal language necessary to abrogate the qualified immunity defense”). On the
19 contrary, the statutes and their legislative history bespeak a strong policy consistent with the
20 policies that inspired the common-law immunities.

21 The common-law immunities grew out of a recognition that telecommunications
22 carriers should not be subject to civil liability for cooperating with government officials
23 conducting surveillance activities. That is true whether or not the surveillance was lawful,
24 so long as the government officials requesting cooperation assured the carrier that it was.

25 *Smith v. Nixon*, 606 F.2d 1183, 1191 (D.C. Cir. 1979), illustrates the point. Hedrick
26 Smith, a reporter for *The New York Times*, sued President Nixon, Henry Kissinger and
27 others, including the Chesapeake & Potomac Telephone Company (“C&P”), for tapping his
28 telephone; the taps were part of an investigation by the White House “plumbers” of

1 suspected leaks. The D.C. Circuit reversed the dismissal of claims against the government
2 officials but affirmed the dismissal of claims against C&P, which had installed the wiretap
3 at the request of government officials acting without a warrant. The court rejected the
4 Smiths' claims against C&P out of hand, adopting the district court's reasoning that the
5 telephone company's "'limited technical role in the surveillance as well as its reasonable
6 expectation of legality cannot give rise to liability for any statutory or constitutional
7 violation.'" *Id.* at 1191 (quoting *Smith v. Nixon*, 449 F. Supp. 324, 326 (D.D.C. 1978)); *see*
8 *also id.* (noting that "the telephone company did not initiate the surveillance"). The
9 reasoning derived from the district court's earlier decision in *Halperin v. Kissinger*, 424 F.
10 Supp. 838, 846 (D.D.C. 1976), *rev'd on other grounds*, 606 F.2d 1192 (D.C. Cir. 1979),
11 where the court rejected similar claims against a telephone company arising out of the same
12 surveillance program. The court relied on the fact that the telephone company "played no
13 part in selecting any wiretap suspects or in determining the length of time the surveillance
14 should remain," and that it "overheard none of plaintiffs' conversations and was not
15 informed of the nature or outcome of the investigation." *Id.*

16 This common-law immunity reflects the fact that carriers merely facilitate
17 government-conducted surveillance (rather than engage in surveillance themselves) and
18 would be reluctant to cooperate with the government if they could be sued for doing so.
19 "[T]o deny the [sovereign] privilege to those who assist federal officers would conflict with
20 the underlying policy of the privilege itself: to remove inhibitions against the fearless,
21 vigorous, and effective administration of policies of government." *Fowler v. Southern Bell*
22 *Tel. & Tel. Co.*, 343 F.2d 150, 157 (5th Cir. 1965) (recognizing defense to civil liability for
23 telecommunications carrier); *see also Craska v. New York Tel. Co.*, 239 F. Supp. 932, 936
24 (N.D.N.Y. 1965) (recognizing defense based on "the common sense analysis that must be
25 made of the undisputed minor part the defendant company played in this situation").

26 The FAC describes a classic situation for applying the immunity recognized in
27 *Smith* and *Halperin*. The FAC alleges that AT&T merely had a limited, technical role in
28 facilitating *the government's* surveillance pursuant to a program "the government had

1 instituted” FAC ¶ 3. The core allegation against AT&T is that it “opened its key
2 telecommunications facilities and databases to direct access *by the NSA and/or other*
3 *government agencies*, intercepting and disclosing *to the government* the contents of its
4 customers’ communications as well as detailed communications records.” FAC ¶ 6
5 (emphasis added); *id.* ¶¶ 42-47 (alleging that AT&T has and is providing “the government”
6 with access to transmitted communications through the use of interception devices such as
7 pen registers); *id.* at ¶¶ 48-64; (alleging that AT&T has and is providing “the government”
8 with access to databases containing stored communications records). This is exactly the
9 sort of alleged activity that federal courts found non-actionable in *Smith* and *Halperin*:
10 taking actions, at the government’s direction, that merely allow government surveillance to
11 be conducted through the carrier’s facilities. The FAC does *not* allege that AT&T selected
12 the targets of the government’s surveillance, determined how long the surveillance would
13 last, overheard conversations, or was told of the nature or outcome of the government’s
14 investigation. Accordingly, the FAC’s allegations against AT&T, even assuming they were
15 true, fall squarely within the immunity recognized by *Smith* and *Halperin*.

16 The FAC also demonstrates that, even assuming the actions alleged, AT&T would
17 have had a “reasonable expectation” that they were authorized. It alleges that “[t]he
18 President has stated that he authorized the Program in 2001, that he has reauthorized the
19 Program more than 30 times since its inception, and that he intends to continue doing so.”
20 FAC ¶ 33. It alleges that “the government instigated, directed and/or tacitly approved all of
21 the above-described acts of AT&T Corp.” and that “AT&T Corp. had at all relevant times a
22 primary or significant intent to assist or purpose of assisting the government in carrying out
23 the Program and/or other government investigations.” FAC ¶¶ 82, 84; *see also id.* ¶¶ 94, 95
24 (alleging that AT&T’s actions were “under color of law”). The FAC thus alleges the type
25 of cooperation that the common-law immunity is designed to protect and encourage.

26 **3. The FAC establishes AT&T’s qualified immunity as a matter of law.**

27 Even if the plaintiffs had not failed to plead the required absence of the absolute
28 immunity afforded by statute and common law, AT&T would, on the facts as alleged in the

1 FAC, be entitled to qualified immunity as a matter of law.⁹ Federal courts have recognized
2 that qualified immunity is available in addition to statutory immunity under the ECPA. *See*
3 *Tapley*, 211 F.3d at 1216 (“[t]he Federal Wiretap Act lacks the specific, unequivocal
4 language necessary to abrogate the qualified immunity defense”); *Blake v. Wright*, 179 F.3d
5 1003, 1011-13 (6th Cir. 1999).¹⁰ Under the doctrine of qualified immunity, “government
6 officials performing discretionary functions generally are shielded from liability for civil
7 damages insofar as their conduct does not violate clearly established statutory or
8 constitutional rights of which a reasonable person would have known.” *Harlow v.*
9 *Fitzgerald*, 457 U.S. 800, 818, 102 S. Ct. 2727 (1982).

10 Qualified immunity also is available to private parties alleged to have assisted the
11 government in performing traditional governmental functions. The availability of
12 immunity for private parties is determined by analyzing two issues: (1) whether there is “a
13 historical tradition of immunity for private parties carrying out” the functions at issue; and
14 (2) “[w]hether the immunity doctrine’s purposes warrant immunity” for the private parties.
15 *Richardson v. McKnight*, 521 U.S. 399, 407, 117 S. Ct. 2100 (1997) (emphasis in original).
16 These factors both confirm that qualified immunity is available to AT&T here.

17 *First*, federal courts have recognized a common-law immunity from suit that applies
18 to telecommunications carriers that cooperate with government officials conducting
19 warrantless surveillance. *See* page 13 above.

20

21 ⁹ Qualified immunity can be established as a matter of law on a motion to dismiss. *E.g.*,
22 *Rush v. FDIC*, 747 F. Supp. 575, 579-80 (N.D. Cal. 1990). The Supreme Court
23 “repeatedly ha[s] stressed the importance of resolving [qualified] immunity questions at
the earliest possible stage in litigation.” *Hunter v. Bryant*, 502 U.S. 224, 227, 112 S. Ct.
534 (1991).

24 ¹⁰ *But see Berry v. Funk*, 146 F.3d 1003, 1013-14 (D.C. Cir. 1998) (qualified immunity not
25 available for ECPA claims). The courts in *Tapley* and *Blake* declined to follow *Berry*
26 because they correctly concluded that it made no sense to “infer that Congress meant to
abolish in the Federal Wiretap Act that extra layer of protection qualified immunity
27 provides for public officials simply because it included an extra statutory defense
available to everyone.” *Tapley*, 211 F.3d at 1216; *see also Blake*, 179 F.3d at 1012. In
28 addition, the *Berry* court did not address the principle that qualified immunity can only be
abolished by specific and unequivocal statutory language. *See Tapley*, 211 F.3d at 1216.

1 *Second*, the purposes of qualified immunity are served by affording AT&T
2 immunity on the facts alleged here. Those purposes are: (1) to protect “government’s
3 ability to perform its traditional functions by providing immunity where necessary to
4 preserve the ability of government officials to serve the public good”; (2) “to ensure that
5 talented candidates [are] not deterred by the threat of damages suits from entering public
6 service”; and (3) to protect “the public from unwarranted timidity on the part of public
7 officials” by minimizing the threat of civil liability. *Richardson*, 521 U.S. at 408 (internal
8 quotation marks and citations omitted). Here, even assuming AT&T engaged in the
9 conduct alleged by the plaintiffs, all of these purposes strongly support qualified immunity
10 for AT&T. Conducting surveillance to preserve national security is a traditional
11 governmental function of the highest importance. In an electronic era, such surveillance
12 may require the facilities of private companies that control critical telecommunications
13 infrastructure. Yet carriers would be reluctant to furnish the required assistance if they
14 were exposed to civil liability while the government officials actually ordering the
15 surveillance were cloaked with qualified immunity. It would make little sense to protect
16 the principal but not his agent.¹¹

17
18

19 ¹¹ *Richardson* presented the question whether prison guards employed by a private prison
20 management firm could assert qualified immunity to a section 1983 suit brought by
21 prisoners who alleged that the guards had injured them. The Supreme Court denied
22 immunity, concluding that there is no tradition of immunity for private prison guards and
23 that the private prison managers were “systematically organized” to assume a major
24 governmental function, “for profit” and “in competition with other firms.” *Richardson*,
25 521 U.S. at 405-07, 408-13. In marked contrast, AT&T is part of an industry traditionally
26 immune from liability for assisting the government. Moreover, AT&T is not in the
27 business of surveillance and does not aspire to perform traditional government functions
28 such as espionage. Finally, unlike the private prison guards, AT&T is alleged to be
“serving as an adjunct to government in an essential governmental activity” and “acting
under close official supervision”—the precise context in which the Court suggested that
qualified immunity may be available to private parties. *Id.* at 409, 413. AT&T’s alleged
situation is far closer to that of the citizen who helps law enforcement officials, a situation
in which the federal courts have held that qualified immunity can be available to private
parties. *See Mejia v. City of New York*, 119 F. Supp. 2d 232, 268 (E.D.N.Y. 2000)
(citizen assisting in making an arrest); *Calloway v. Boro of Glassboro*, 89 F. Supp. 2d
543, 557 n.21 (D.N.J. 2000) (sign language interpreter during a police interrogation).

1 Where qualified immunity is available, a two-part analysis determines whether a
2 defendant is entitled to it. The court must determine: (1) “whether the plaintiff has alleged
3 a violation of a right that is clearly established”; and (2) “whether, under the facts alleged, a
4 reasonable official could have believed that his conduct was lawful.” *Collins v. Jordan*,
5 110 F.3d 1363, 1369 (9th Cir. 1996).

6 Under the first prong of the analysis, AT&T’s alleged conduct does not violate any
7 clearly established constitutional or statutory right. If the past several months’ public
8 debate, congressional debate, and legal argumentation over the Program demonstrates
9 anything, it is that the legality of the Program is the subject of reasonable disagreement
10 among well-intentioned and capable lawyers. Indeed, the Supreme Court has specifically
11 reserved the question whether the President has inherent constitutional authority to engage
12 in warrantless foreign intelligence surveillance, *see United States v. United States District*
13 *Court (Keith)*, 407 U.S. 297, 308, 321-22 & n.20 (1972), and the courts of appeals have
14 unanimously held, even after the passage of FISA, that he does. *See, e.g., In re Sealed*
15 *Case*, 310 F.3d at 742 (collecting cases). As such, even if AT&T’s alleged conduct could
16 be directly equated with that of the government – which it cannot – AT&T’s alleged
17 conduct could not amount to “a violation of a right that is clearly established.” *Id.*

18 Second, nothing alleged in the FAC suggests that AT&T’s alleged conduct was
19 carried out in bad faith, *i.e.*, that it did not reasonably believe that any alleged conduct was
20 lawful. The FAC alleges that the President authorized and reauthorized the government
21 surveillance program, that “the government instigated, directed and/or tacitly approved” all
22 of AT&T’s alleged actions, and that AT&T “had at all relevant times a primary or
23 significant intent to assist or purpose of assisting the government in carrying out the
24 Program and/or other government investigations.” *Id.* ¶¶ 33, 82, 84. These allegations
25 demonstrate that, even if AT&T had done what the FAC alleges, it would have had a
26 reasonable belief in the legality of its alleged conduct. Therefore, AT&T is entitled to
27 qualified immunity from suit as a matter of law.

28

1 **B. PLAINTIFFS LACK STANDING.**

2 Under Article III of the Constitution, federal courts have the power to adjudicate
3 only actual “cases” and “controversies.” “The several doctrines that have grown up to
4 elaborate that requirement are founded in concern about the proper—and properly
5 limited—role of the courts in a democratic society,” and “[t]he Art. III doctrine that
6 requires a litigant to have ‘standing’ to invoke the power of a federal court is perhaps the
7 most important of these doctrines.” *Allen v. Wright*, 468 U.S. 737, 750, 104 S. Ct. 3315
8 (1984) (citations omitted).

9 Plaintiffs must establish both constitutional and prudential standing. To establish
10 constitutional standing, plaintiffs must demonstrate (among other things) that they suffered
11 “an injury in fact” that is “concrete and particularized” and “actual or imminent.” *Lujan v.*
12 *Defenders of Wildlife*, 504 U.S. 555, 560-61, 112 S. Ct. 2130 (1992). In the context of a
13 class action, the named plaintiffs “must allege and show that they personally have been
14 injured, not that injury has been suffered by other, unidentified members of the class to
15 which they belong and which they purport to represent.” *Warth v. Seldin*, 422 U.S. 490,
16 502 (1975); *see also O’Shea v. Littleton*, 414 U.S. 488, 494 (1974) (unless named plaintiffs
17 have standing individually, “none may seek relief on behalf of himself or any other member
18 of the class”); *Hodgers-Durgin v. de la Vina*, 199 F.3d 1037, 1045 (9th Cir. 1999) (en banc)
19 (“Any injury unnamed members of this proposed class may have suffered is simply
20 irrelevant . . .”). To establish prudential standing, plaintiffs also must show that their
21 situation differs from that of the public generally. *See Valley Forge Christian College v.*
22 *Americans United for Separation of Church and State, Inc.*, 454 U.S. 464, 474-75, 102 S.
23 Ct. 752 (1982). The standing inquiry must be “especially rigorous” where, as here,
24 “reaching the merits of the dispute would force [a court] to decide whether an action taken
25 by one of the other two branches of the Federal Government was unconstitutional.”
26 *Raines v. Byrd*, 521 U.S. 811, 819-20 (1997).

27
28

1 **1. Plaintiffs have not sufficiently alleged injury-in-fact.**

2 The standing requirement ““focuses on the party seeking to get his complaint before
3 a federal court and not on the issues he wishes to have adjudicated.”” *Valley Forge*
4 *Christian College*, 454 U.S. at 484 (quoting *Flast v. Cohen*, 392 U.S. 83, 99, 88 S. Ct. 1942
5 (1968)). Thus, the named plaintiffs’ first task is to allege facts showing that *they* have
6 suffered injury in fact. This they have failed to do.

7 In relation to both the Program and the related “data-mining” allegations, the FAC
8 alleges in wholly conclusory terms that plaintiffs’ communications have been or will be
9 “disclosed” to the government, or that AT&T has provided some form of “access” to
10 various databases or datastreams to the government. *See, e.g.*, FAC ¶ 52 (“On information
11 and belief, AT&T Corp. has disclosed and is currently disclosing to the government records
12 concerning communications to which Plaintiffs and class members were a party”); *id.* ¶ 61
13 (“On information and belief, AT&T Corp. has provided the government with direct access
14 to the contents” of various databases that include generic categories information pertaining
15 to plaintiffs); *see also id.* ¶¶ 6, 63, 64, 81, 97, 103, 105, 107, 113, 121, 128, 141. But the
16 FAC alleges only that plaintiffs are (or were) AT&T customers who on occasion make
17 international telephone calls or surf the Internet. FAC ¶¶ 13-16. No allegation suggests
18 that plaintiffs ever communicated with terrorists or with al Qaeda—or gave the government
19 reason to think they had. Indeed, the FAC expressly excludes from the class plaintiffs
20 purport to represent “anyone who knowingly engages in sabotage or international terrorism,
21 or activities that are in preparation therefore.” *Id.* ¶ 70. Absent some concrete allegation
22 that the government monitored their communications or records, all plaintiffs really have is
23 a suggestion that AT&T provided a means by which the government *could have done so*
24 had it wished. This is anything but injury-in-fact.¹²

25

26 ¹² In their injunction papers, plaintiffs implicitly acknowledge that they cannot allege that
27 any “human beings personally read or listen to the acquired communications” but claim it
28 does not matter. Pl. Mem. in Support of Motion for Prelim. Inj. at 17. That is incorrect.
None of the cases cited by plaintiffs is a standing case; all pertain only to the substantive
(continued...)

1 To establish standing, a complaint’s allegations must be *factual*. See *Lujan*,
2 504 U.S. at 561. Unsupported conclusions and unwarranted inferences will not suffice.
3 Plaintiffs assert a belief that their communications have somehow been divulged to the
4 government, but they allege no specific facts suggesting that government agents might have
5 targeted them or their communications. The FAC is thus far weaker than other complaints
6 filed by plaintiffs who, while failing to establish standing, at least could muster facts
7 suggesting a governmental interest in their activities.

8 In *United Presbyterian Church v. Reagan*, 738 F.2d 1375, 1380-81 (D.C. Cir.
9 1984), for example, the plaintiffs included a number of stalwarts of the Vietnam antiwar
10 movement and the civil rights movement, such as the former Stokeley Carmichael. *Id.* at
11 1381 n.2. They alleged that they had been or currently were subject to unlawful
12 surveillance, frequently traveled abroad, and were particularly likely to be found to be
13 agents of foreign powers. *Id.* at 1380. Nonetheless, the D.C. Circuit, in an opinion by then-
14 Judge Scalia, held that these activists could not establish standing to challenge Executive
15 Order No. 12333, entitled “United States Intelligence Activities,” because they could not
16 show they were subject to surveillance conducted under that Order. Similarly, in *Halkin v.*
17 *Helms*, 690 F.2d 977 (D.C. Cir. 1982), the plaintiffs were antiwar activists who claimed that
18 their communications had been intercepted. *Id.* at 981 n.3. Because they failed to provide
19 factual support for this claim, however, the court held that they lacked standing to challenge
20 government intelligence-gathering activities, including the CIA’s “Operation CHAOS.”
21 The sole difference between the FAC and these complaints (beyond the fact that the
22 plaintiffs there were noted activists) is that the plaintiffs here use the magic words “on

23 (...continued)
24 scope of liability where plaintiffs’ own communications had undoubtedly been monitored
25 and standing was clear. In *Jacobson v. Rose*, 592 F.2d 515 (9th Cir. 1978), for example,
26 the plaintiffs were individuals whose communications had actually been monitored by
27 government agents; class action status was denied, and the district court limited the
28 plaintiffs to those whose conversations had allegedly been overheard. See *id.* at 518.
Nonetheless, the Ninth Circuit reversed a verdict against the phone company. Although
the court said that “the victim’s privacy is violated, regardless of which particular
individuals actually listen to the tapes,” *id.*, it never suggested that standing exists where
there is no allegation that *anyone* has listened.

1 information and belief’ to allege that AT&T has intercepted and disclosed their
2 communications to the government. But that is legally insufficient.

3 Nor can plaintiffs establish standing through the common tactic of alleging that the
4 Program (or AT&T’s alleged involvement) has “chilled” constitutionally-protected
5 activities. Although plaintiffs do not allege “chill” in the FAC, their preliminary injunction
6 papers suggest that at least named-plaintiff Jewel asserts a “chill” on her speech. *See* Pl.
7 Mem. in Support of Mot. for Prelim. Inj. at 25-26. This is precisely the kind of abstract
8 injury that the federal courts have consistently held is insufficient to create standing to
9 challenge a government surveillance program. In *Laird v. Tatum*, 408 U.S. 1, 13-15, 92 S.
10 Ct. 2318 (1972), the plaintiffs were held not to have standing to challenge the Army’s
11 domestic surveillance of peaceful, civilian activity based on alleged “chill” because
12 “[a]llegations of a subjective ‘chill’ are not an adequate substitute for a claim of specific
13 present objective harm or a threat of specific future harm.” *Id.* at 13-14. As the D.C.
14 Circuit explained, “[a]ll of the Supreme Court cases employing the concept of ‘chilling
15 effect’ involve situations in which the plaintiff has unquestionably suffered some concrete
16 harm (past or immediately threatened) apart from the ‘chill’ itself. . . . ‘Chilling effect’ is
17 cited as the *reason* why the governmental imposition is invalid rather than as the *harm*
18 which entitles the plaintiff to challenge it.” *United Presbyterian*, 738 F.2d at 1378
19 (citations omitted, emphasis original). In cases like this one that do not involve an
20 “exercise of governmental power [that is] regulatory, proscriptive, or compulsory in
21 nature,” *Laird*, 408 U.S. at 11, “mere subjective chilling effects,” such as those asserted by
22 the plaintiffs, “are simply not objectively discernable and are therefore not constitutionally
23 cognizable.” *Vernon v. City of Los Angeles*, 27 F.3d 1385, 1395 (9th Cir. 1994); *see also*
24 *Donohoe v. Duling*, 465 F.2d 196, 201-02 (4th Cir. 1972).

25 **2. Plaintiffs’ dissatisfaction with government policy does not give them standing.**

26 The FAC is, at its core, founded on disagreement with the government’s Terrorist
27 Surveillance Program. Plaintiffs’ interest in resolving this issue is no greater than that of
28 any other citizen who disagrees with the government’s conduct. In a democracy, this kind

1 of complaint is resolved by the political process, not the courts, especially not in a suit
2 against a private third-party. "Vindicating the *public* interest (including the public interest
3 in Government observance of the Constitution and laws) is the function of Congress and the
4 Chief Executive." *Lujan*, 504 U.S. at 576 (emphasis in original). Courts should address
5 such issues only as a last resort, and then only if an actual case or controversy is presented
6 by a plaintiff who incurs an injury that differs from that incurred by dissatisfied citizens in
7 general. *Valley Forge Christian College*, 454 U.S. at 473. "[A] plaintiff raising only a
8 generally available grievance about government – claiming only harm to his and every
9 citizen's interest in proper application of the Constitution and laws, and seeking relief that
10 no more directly and tangibly benefits him than it does the public at large – does not state
11 an Article III case or controversy." *Lujan*, 504 U.S. at 574-75.

12 Plaintiffs may sincerely believe that the Program is illegal and unconstitutional, but
13 that belief is not sufficient to create standing. Chief Justice Burger's observation in *Laird v.*
14 *Tatum* is particularly appropriate here:

15 Stripped to its essentials, what respondents appear to be seeking is a broad-
16 scale investigation, conducted by themselves as private parties armed with
17 the subpoena power of a federal district court and the power of cross-
18 examination, to probe into the Army's intelligence-gathering activities . . .
19 Carried to its logical end, this approach would have the federal courts as
20 virtually continuing monitors of the wisdom and soundness of Executive
21 action.

22 *Laird*, 408 U.S. at 14-15.

23 The Supreme Court has voiced these concerns on a number of occasions. *See also*,
24 *e.g.*, *Allen*, 468 U.S. at 750-61; *City of Los Angeles v. Lyons*, 461 U.S. 95, 111-12, 103 S.
25 Ct. 1660 (1983); *Schlesinger v. Reservists Committee to Stop the War*, 418 U.S. 208, 220-
26 23, 94 S. Ct. 2925 (1974); *O'Shea*, 414 U.S. 488, 492-95, 94 S. Ct. 669 (1974). Article III
27 courts are tribunals of limited jurisdiction, not vehicles for publicizing political conflicts or
28 roving commissions to enable more discovery or public disclosure of sensitive or classified
government programs than the Freedom of Information Act allows.

These concerns are at their apex when a plaintiff seeks to probe the executive's
conduct of foreign affairs. As this Court said in *In re World War II Era Japanese Forced*

1 *Labor Litig.*, 164 F. Supp. 2d 1160, 1170 (N.D. Cal. 2001), “[t]he Supreme Court has long
2 acknowledged the federal government’s broad authority over foreign affairs” and “observed
3 that the Constitution entrusts ‘the field of foreign affairs . . . to the President and the
4 Congress.’” (citations omitted).

5 For good reason, courts are loath to interfere with issues firmly within the province
6 of the legislative and executive branches of government. Public accounts of the Terrorist
7 Surveillance Program indicate that the executive branch uses it to gather foreign
8 intelligence and time-sensitive counterterrorism information and that it was approved by the
9 government’s most senior legal officials. Indeed, Congress is now reviewing this
10 understanding. *See, e.g.*, Terrorist Surveillance Act of 2006, S. 2455, 109th Cong., 2d Sess.
11 (introduced March 16, 2006). Few issues are less suited to judicial resolution than an
12 ongoing national policy dispute concerning the propriety of foreign intelligence activities.

13 **3. Plaintiffs fail to allege concrete injuries to their statutory interests.**

14 To have standing, a plaintiff must allege a concrete and personal stake in the
15 outcome of a lawsuit. The constitutional requirement of injury-in-fact is no less applicable
16 when violation of a statute is alleged. *O’Shea v. Littleton*, 414 U.S. at 493-94 (citing
17 *Baker v. Carr*, 369 U.S. 186, 204, 82 S. Ct. 691, 703 (1962); *United States v. SCRAP*,
18 412 U.S. 669, 687, 93 S. Ct. 2405, 2415 (1973)). “[S]tatutes do not purport to bestow the
19 right to sue in the absence of any indication that invasion of the statutory right has occurred
20 or is likely to occur.” *O’Shea*, 414 U.S. at 495 n.2.

21 Plaintiffs lack standing to assert their statutory claims (Counts II-VII) because the
22 FAC alleges no *facts* suggesting that their statutory rights have been violated. For example,
23 Count II asserts a claim under the criminal and civil liability provisions of the Foreign
24 Intelligence Surveillance Act (“FISA”), 50 U.S.C. §§ 1809, 1810. Plaintiffs allege “on
25 information and belief” that AT&T has installed or helped to install “interception devices
26 and pen registers and/or trap and trace devices” and conclude that AT&T has conducted
27 “electronic surveillance” (as defined in 50 U.S.C. § 1801). FAC ¶¶ 43, 93-94. But even if
28 true, these allegations are insufficient to establish that plaintiffs themselves suffered any

1 definite injury sufficient to entitle them to represent the class of individuals whose
2 communications they allege to have been intercepted. Plaintiffs' own allegations do not
3 make the facially absurd claim that *all* AT&T customers have been subjected to
4 surveillance by the government,¹³ and the FAC alleges nothing to suggest that the *named*
5 *plaintiffs* were themselves subject to surveillance. Because the named plaintiffs do not
6 allege facts demonstrating that, under the applicable FISA definitions, the government
7 actually acquired the content of their own communications,¹⁴ they are without standing.
8 The other counts of the FAC fare no better.¹⁵

9 **IV. CONCLUSION.**

10 For the foregoing reasons, the Amended Complaint should be dismissed.

11 Dated: April 28, 2006.

12 //

13 //

14 //

15

16

17

18 ¹³ For example, plaintiffs allege that interception devices “acquire the content of all *or a*
19 *substantial number of* the wire or electronic communications transferred through the
20 AT&T Corp. facilities *where they have been installed*” (emphasis added). FAC ¶ 44.
21 Similar allegations appear in ¶ 45 with respect to the use of pen registers and trap and
22 trace devices. Thus, plaintiffs appear to allege that some AT&T customers were not
23 subject to the surveillance alleged in the FAC: not all, but only a “substantial number” of
24 communications transferred by AT&T Corp. may have been subject to surveillance, and
25 only communications passing through certain facilities are even alleged to have been
26 subject to surveillance. Moreover, there is no allegation regarding whether or how the
27 government actually reviews or uses the data, if at all.

28 ¹⁴ Nor could they, as the facts necessary to support such an allegation would, even if they
existed, be classified and legally unavailable to any private party, including AT&T.

¹⁵ Counts III, IV, V and VI parrot the relevant statutory language, but no facts buttress the
legal conclusions that plaintiffs recite, and no actual injury is alleged. Plaintiffs’
allegation of unfair competition in violation of California Business and Professions Code
§ 17200 has the further standing flaw that plaintiffs failed to allege facts indicating that
they “suffered injury in fact and . . . lost money or property as a result of such unfair
competition.” Cal. Bus. & Prof. Code §17204. Indeed, there is no suggestion that they
did not receive the telecommunications services for which they paid.

1 PILLSBURY WINTHROP
SHAW PITTMAN LLP
2 BRUCE A. ERICSON
DAVID L. ANDERSON
3 JACOB R. SORENSEN
MARC H. AXELBAUM
4 BRIAN J. WONG
50 Fremont Street
5 Post Office Box 7880
San Francisco, CA 94120-7880

SIDLEY AUSTIN LLP
DAVID W. CARPENTER
DAVID L. LAWSON
BRADFORD A. BERENSON
EDWARD R. MCNICHOLAS
1501 K Street, N.W.
Washington, D.C. 20005

6 By /s/ Bruce A. Ericson
7 Bruce A. Ericson

By /s/ Bradford A. Berenson
Bradford A. Berenson

8
9 Attorneys for Defendants AT&T CORP. and AT&T INC.

10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28