ELECTRONIC FRONTIER FOUNDATION
CINDY COHN (145997)
cindy@eff.org
LEE TIEN (148216)
tien@eff.org
KURT OPSAHL (191303)
kurt@eff.org
KEVIN S. BANKSTON (217026)
bankston@eff.org
CORYNNE MCSHERRY (221504)
corynne@eff.org
JAMES S. TYRE (083117)
jstyre@eff.org
454 Shotwell Street
San Francisco, CA 94110
Telephone: 415/436-9333
415/436-9993 (fax)

Attorneys for Plaintiffs

[Additional counsel appear on signature page.]

UNITED STATES DISTRICT COURT

FOR THE NORTHERN DISTRICT OF CALIFORNIA

SAN FRANCISCO DIVISION

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

Plaintiffs,

v.

AT&T CORP., et al.,

Defendants.

No. C-06-0672-VRW

CLASS ACTION

PLAINTIFFS' OPPOSITION TO MOTION TO DISMISS AMENDED COMPLAINT BY DEFENDANT AT&T, CORP.

Date: June 23, 2006
Time: 9:30 a.m.
Courtroom: 6, 17th Floor
Judge: Hon. Vaughn Walker

Filed concurrently:
1. Proposed Order
2. Motion to Extend Page Limits

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Other Authorities

Law Review Articles and Treatises

ISSUES TO BE DECIDED

1. Is there a justiciable case or controversy before this Court where plaintiffs have suffered and alleged a concrete injury as a result of AT&T's ongoing wholesale and illegal surveillance of their communications and disclosure of their records?

2. May AT&T continue to violate the established federal and state rights of millions of its customers by merely raising the possibility that the government provided it with some purported authorization to do so?

3. Should the Court create *sua sponte* an entirely new and unprecedented category of common law absolute or qualified immunity for AT&T, to excuse it from blatant violations of federal and state law?

MEMORANDUM OF POINTS AND AUTHORITIES

I. STATEMENT OF FACTS AND SUMMARY OF ARGUMENT

This case is a class action brought on behalf of all residential customers and subscribers of defendants AT&T Corp. and AT&T Inc. Plaintiffs allege that defendants are violating a number of federal and California statutes and, as agents of the government, the First and Fourth Amendments.[1] They do so by intercepting and disclosing to the National Security Agency ("NSA") the domestic and international communications of millions of Americans, as well as by disclosing their entire databases of phone and Internet records, including those communications and records of plaintiffs.

Plaintiffs further allege that defendants have received no court order or other judicial authorization for their wholesale surveillance, and that defendants have received no other lawful authorization that comports with the procedures of the Foreign Intelligence Surveillance Act of 1978 ("FISA"), 50 U.S.C. §§ 1801, *et seq.*, or Title III of the Omnibus Crime Control and Safe Streets Act of 1968 ("Title III"), 18 U.S.C. §§ 2511 *et seq.*, which are the exclusive means by which the government may domestically intercept or conduct electronic surveillance on wire or electronic communications. 18 U.S.C. § 2511(2)(f).

Specifically, Plaintiffs' Amended Complaint ("Complaint," Dkt 8) alleges, *inter alia*, an "illegal collaboration" between Defendant AT&T Corp. ("AT&T") and the government, Complaint ¶ 8, whereby "AT&T [ ] has opened its key telecommunications facilities and databases to direct access by the NSA and/or other government agencies, intercepting and disclosing to the government the contents of its customers' communications as well as detailed communications records about millions of its customers, including Plaintiffs and class members." *Id.* at ¶ 6. AT&T's unauthorized cooperation with the government is "without judicial or other lawful authorization," *id.* at ¶ 81, and was undertaken "intentionally, with deliberate indifference, or with reckless disregard of, Plaintiffs' and class members' constitutional rights," *id.* at ¶ 87, "willful[ly]

[1] Specifically, plaintiffs allege statutory violations including without limitation: 50 U.S.C. § 1809, 18 U.S.C. § 2511, 47 U.S.C. § 605 and 18 U.S.C. § 2702 on behalf of a nationwide class and allege all of those plus a violation of Cal. Bus. & Prof. Code § 17200 on behalf of the California sub-class.

and for purposes of direct or indirect commercial advantage or private financial gain." *Id*. at ¶ 114.

AT&T's conduct is part of an NSA surveillance program ("the Program") far broader than the so-called "Terrorist Surveillance Program" initially admitted by the government, which the government and AT&T contend is limited to international communications in which there is a reasonable suspicion that either the sender or the receiver is connected to Al Qaeda. AT&T Corp. Mot. to Dismiss ("MTD") (Dkt 86), at 3. This broader Program, the existence of which has been widely reported and of which plaintiffs have provided evidence under seal, "intercepts millions of communications made or received by people inside the United States," Complaint ¶ 39, and "collects . . . a vast amount of communications traffic data." *Id*. at ¶ 40. As the Complaint further alleges, AT&T is providing "large volumes of domestic and international telephone and Internet traffic" to the broader Program by intercepting and disclosing to the NSA the "streams of domestic, international and foreign telephone and Internet communications" transmitted through its "key telecommunications facilities," *id*. at ¶¶ 38, 42-43, and by disclosing the contents of its entire database of phone call and Internet records. *Id*. at ¶¶ 51-52, 61.

The complaint does not allege that these interceptions and disclosures have been targeted at plaintiffs as potential terrorist threats or suspects; rather, the entire thrust of the complaint is that AT&T and the government's illegal collaboration is *untargeted*, such that plaintiffs' communications were and are intercepted for the government, and their records disclosed to the government, indiscriminately. The gravamen of the Complaint is not that plaintiffs have some unspecified fear that they *may* have been wrongfully ensnared in the Terrorist Surveillance Program, as AT&T claims. Instead, it alleges that plaintiffs' *have already been* ensnared in the broader Program's fishing expedition through the entirety of AT&T's networks and databases. The Complaint therefore alleges a concrete injury to plaintiffs' statutory and constitutional rights and presents a clear case and controversy.

AT&T also uses a straw man argument to contend that plaintiffs failed to plead the absence of "blanket immunity" under statute. There are three reasons why this argument fails. First, Congress has not established such a heightened pleading requirement; rather, to avoid liability, it is AT&T's burden to show that its conduct is in accord with a valid court order or certification

authorized by statute that it has relied upon in good faith. Second, even if there were a requirement that plaintiffs allege AT&T's conduct as being in bad faith and without good faith reliance on any valid court order or certification, as AT&T argues, the allegations in the Complaint already satisfy it. Finally, Congress has plainly not authorized or immunized the surveillance alleged here, which goes far beyond the limits of Title III and FISA.

AT&T's claims that some form of common law absolute or qualified immunity excuses its illegal conduct are equally baseless. Not only are the doctrines inapplicable to a private corporation's violations of clearly established constitutional and statutory restrictions on surveillance, they are superceded by Congress' statutory defenses. Moreover, even if somehow applicable, neither doctrine can require the dismissal of plaintiffs' equitable claims. Therefore, AT&T's motion to dismiss must be denied.[2]

II. STANDARDS FOR DECIDING THIS MOTION

"On a motion to dismiss, all well-pleaded allegations of material fact are taken as true and construed in a light most favorable to the non-moving party." *Wyler Summit P'ship v. Turner Broad. Sys., Inc.*, 135 F.3d 658, 661 (9th Cir. 1998) (citation omitted). The standard is the same for "purposes of ruling on a motion to dismiss for want of standing." *Tyler v. Cuomo*, 236 F.3d 1124, 1131 (9th Cir. 2000). As the Supreme Court has stated, "a complaint should not be dismissed unless 'it appears beyond doubt that the plaintiff can prove no set of facts in support of his claim which would entitle him to relief.'" *McLain v. Real Estate Bd. of New Orleans, Inc.*, 444 U.S. 232, 246 (1980) (citation omitted). Furthermore, courts must assume that all general allegations "embrace whatever specific facts might be necessary to support them," *Peloza v. Capistrano Unified Sch. Dist.*, 37 F.3d 517, 521 (9th Cir. 1994), and courts adopt whatever inference supports a valid claim. *TwoRivers v. Lewis*, 174 F.3d 987, 991 (9th Cir. 1999); *see also Warren v. Fox Family Worldwide, Inc.*, 328 F.3d 1136, 1140 (9th Cir. 2003) (at pleading stage, plaintiffs "need

[2] Co-defendant AT&T Inc. has made a separate motion to dismiss on 12(b)(2) jurisdiction grounds (Dkt 79), and joined in this motion by AT&T Corp. This Opposition applies both to AT&T Corp.'s motion and to AT&T Inc.'s joinder in it.

only show that the facts alleged, if proved, would confer standing upon him." (citations omitted)).[3]

III. ARGUMENT

A. Plaintiffs Have Standing to Seek Redress for AT&T's Unlawful Surveillance.

Plaintiffs have standing because they allege that they (1) have suffered an actual and threatened injury as (2) a result of the putatively illegal conduct of AT&T that (3) "is likely to be redressed by a favorable decision." *Simon v. Eastern Kentucky Welfare Rights Org.*, 426 U.S. 26, 38, 41 (1976); *see also Lujan v. Defenders of Wildlife*, 504 U.S. 555 (1992). The Complaint squarely meets all the standing requirements. For example, the Complaint alleges that:

> On information and belief, AT&T Corp. has opened its key telecommunications facilities and databases to direct access by the NSA and/or other government agencies, intercepting and disclosing to the government the contents of its customers' communications as well as detailed communications records about millions of its customers, *including Plaintiffs and class members*.

Complaint ¶ 6 (emphasis added); *see also id.* at ¶¶ 43, 44, 47, 52, 60, 61, 85, 86, 95, 97, 103, 105, 107, 113, 121, 128, 141. These allegations are more than sufficient to establish plaintiffs' standing.[4]

Specifically, plaintiffs have alleged widespread injury, both actual and threatened, that can be directly traced to AT&T's collaboration with the government's warrantless surveillance Program in violation of the First and Fourth Amendment of the United States Constitution, as well as state and federal statutes. The actual or threatened injury required by Article III may exist solely by virtue of "statutes creating legal rights, the invasion of which creates standing." *Warth v. Seldin*, 422 U.S. 490, 500 (1975). Plaintiffs have alleged facts sufficient for standing under each state and

---

[3] *Warren* also notes that courts may look to extrinsic facts, such as matters of public record, introduced to challenge standing. *Id.* at 1139. While AT&T cites to this proposition (AT&T Motion to Dismiss ("MTD") at 4), it has introduced no facts showing that it did not intercept plaintiffs' communications or disclose their records. Accordingly, AT&T's motion must be treated as a facial, not factual, attack under Fed. R. Civ. P. 12(b)(1).

[4] AT&T attempts to convince this Court to narrowly construe allegations of AT&T's surveillance of "all or a substantial number of" the communications of the plaintiffs and the class as "not all, but only a 'substantial number' of" such communications. MTD at 25. The plain inference from the Complaint, however, is that AT&T is indiscriminately surveilling the communications of all its customers, including plaintiffs. *See Columbia Natural Resources, Inc. v. Tatum*, 58 F.3d 1101, 1109 (6th Cir. 1995) ("When an allegation is capable of more than one inference, it must be construed in the plaintiff's favor.").

federal statute in the Complaint:

- Plaintiffs have standing under 18 USC § 2520 because they have alleged a violation of Title III. *See, e.g.*, Complaint ¶ 108. Unless the surveillance is authorized by 18 U.S.C. § 2511(2)(a)(ii), "any person whose wire, oral, or electronic communication is intercepted, disclosed, or intentionally used in violation of this chapter" has standing to pursue a civil suit under Title III. Not only have plaintiffs alleged interception, disclosure, and intentional use (*see, e.g.*, Complaint ¶¶ 6, 43-44, 46), plaintiffs have alleged the surveillance is without "lawful authorization," Complaint ¶ 81, taking it outside the ambit of Section 2511(2)(a)(ii).[5]
- Plaintiffs have standing under 50 U.S.C. § 1810 because they are aggrieved persons pursuant to FISA. *See*, *e.g.*, Complaint ¶ 98. Pursuant to 50 USC § 1801(k), an "'Aggrieved person' means . . . any . . . person whose communications or activities were subject to electronic surveillance." Plaintiffs are "aggrieved" because they have repeatedly alleged that their communications or activities were subject to electronic surveillance. *See* Complaint ¶¶ 42-63.[6]
- Plaintiffs have standing under 47 U.S.C. § 605(e)(3)(A), because plaintiffs have alleged that AT&T divulged or published their wire and electronic communications in violation of 47 U.S.C. § 605(a). *See* Complaint ¶¶ 6, 46, 52, 64, 113-116. Furthermore, a telephone company's placement of a wiretapping mechanism on a telephone line is an "interception" within the meaning of § 605. *Huff v Michigan Bell Tel. Co*. 278 F. Supp. 76, 77 (E.D.Mich. 1967).

---

[5] As discussed below, such an allegation is not necessary to plead a violation of the statute. However, even assuming that plaintiffs did have to allege that AT&T's conduct was not authorized by 18 U.S.C. § 2511(2)(a)(ii), its pleading on this point was sufficient. *See* Section III.B. *infra*.

[6] This also disposes of any concern about prudential standing. "History associates the word 'aggrieved' with a congressional intent to cast the standing net broadly-beyond the common-law interests and substantive statutory rights upon which 'prudential' standing traditionally rested." *Fed. Election Comm'n v. Akins*. 524 U.S. 11, 12 (1998); s*ee also Dep't of Commerce v. United States House of Representatives*, 525 U.S. 316, 327 (1999) (Congress' use of "any person aggrieved" in the Census Act, 13 U.S.C. § 209(b), "eliminated any prudential concerns in [that] case.")

- Plaintiffs have standing under 18 U.S.C. § 2707, because they have alleged that they were "aggrieved by [AT&T's] violation of [18 U.S.C. § 2702] in which the conduct constituting the violation [was] engaged in with a knowing or intentional state of mind." 18 U.S.C. § 2707(a); *see* Complaint ¶¶ 119-132. For example, plaintiffs have alleged that AT&T divulged their call detail records to the government (Complaint ¶¶ 52-61), as was recently confirmed by reporting in USA Today. *See* Leslie Cauley, *NSA has massive database of Americans' phone calls*, USA Today, May 11, 2006, at p. A1.
- Plaintiffs have standing under Calif. Bus. & Prof. Code § 17200 *et seq*. because they have alleged injury (lost money and property in the form of fees paid, Complaint ¶ 147) due to AT&T's unfair, unlawful and/or fraudulent business practices described above. In addition to the statutory and constitutional violations described above, plaintiffs have alleged two more violations of law that comprise an unlawful business practice under California law: installation of unauthorized pen registers and tap and trace devices (Complaint ¶¶ 43, 140) and unauthorized disclosure of customer proprietary network information (Complaint ¶¶ 53-61) that AT&T obtained by virtue of its provision of telecommunications services. *See* Complaint ¶¶ 138-147. Moreover, plaintiffs have alleged a violation of their California Constitutional right to privacy, which is both unfair and unlawful. *See People v. Blair*, 25 Cal. 3d 640, 653-55 (1979) (California Constitutional right to privacy protects telephone records) and *People v. McKunes*, 51 Cal. App. 3d 487, 490-91 (1975) (a person's constitutional right of privacy is violated by the government's obtaining from the telephone company, without having secured a subpoena or other court order, records of telephone calls between that person and a telephone company subscriber); *see also* 86 Ops. Cal. Att'y. Gen. 198, 2003 WL 22996726 at *4 (Dec. 18, 2003) ("[T]he California Constitution allows the placement of pen registers and trap and trace devices [for acquisition of dialing information] only if a judicial ruling is first obtained that the law enforcement officers are entitled to the records.").

In addition to having standing under the above statutes, plaintiffs have also alleged direct

injury to their rights under the First and Fourth Amendments to the United States Constitution, based on AT&T's warrantless and unreasonable search and seizure of communications and records in which plaintiffs have a reasonable expectation of privacy. Complaint ¶¶ 79, 81, 85.[7] These searches and seizures in violation of plaintiffs' Fourth Amendment rights have further violated and chilled their First Amendment rights to speak and receive speech anonymously, and to associate privately. *Id.* at ¶¶ 80, 85; *see, e.g., Katz v. U.S.*, 389 U.S. 347 (1967) (holding electronic voice surveillance to be a "search and seizure"); *Berger v. New York*, 388 U.S. 41, 59 (1967) (same); *Olagues v. Russoniello*, 797 F.2d 1511 (9th Cir. 1986) (*en banc*), vacated as moot, 484 U.S. 806 (1987) (finding standing under First Amendment where plaintiffs subjected to surveillance, distinguishing *Laird v. Tatum*, 408 U.S. 1 (1972)); *Presbyterian Church (U.S.A.) v. U.S.*, 870 F.2d 518 (9th Cir. 1989) (church has First Amendment standing where individual members were chilled).

Attempting to support its straw man arguments, AT&T inappositely cites to a case where the plaintiffs did not specifically allege that they had been subject to surveillance. MTD at 21; *see United Presbyterian Church v. Reagan*, 738 F.2d 1375, 1380 (D.C. Cir. 1984) ("[Appellants] have not adequately averred that any specific action is threatened or even contemplated against them.").[8]

---

[7] Although AT&T is a private party, plaintiffs have alleged agency (Complaint ¶¶ 82-85), and a private party's conduct counts as state action for Fourth Amendment purposes "if the private party act[s] as an instrument or agent of the Government." *Skinner v. Railway Labor Executives' Ass'n*, 489 U.S. 602, 614 (1989); *see also U.S. v. Miller*, 688 F.2d 652, 657 (9th Cir. 1982) (holding that private action counts as government conduct if, at the time of the search, the government knew of or acquiesced in the intrusive conduct, and the party performing the search intended to assist law enforcement efforts).

[8] AT&T attempts to further muddy the waters with a footnote argument, MTD at 20, n.12, claiming that plaintiffs must specifically allege that a person has reviewed plaintiffs' communications before an injury has occurred. However, the statutes clearly establish standing for anyone whose communications have been intercepted or subjected to electronic surveillance, i.e., whose communications have been acquired by a device, without reference to whether they are listened to or read afterwards. *See* 18 U.S.C. § 2510(4) (definition of "intercept" in Title III) and 50 U.S.C. § 1801(f)(2) (relevant definition of "electronic surveillance" in FISA); *see, e.g., U.S. v. Rodriguez*, 968 F.2d 130, 136 (2d Cir. 1992) (holding that "when the contents of a wire communication are captured or redirected in any way, an interception occurs at that time."); *In re State Police Litigation*, 888 F. Supp. 1235, 1264 (D. Conn. 1995) (holding that "it is the act of diverting, and not the act of listening, that constitutes an 'interception.'"); *Jacobson v. Rose*, 592 F.2d 515, 522 (9th Cir. 1978) (same); *U.S. v. Lewis*, 406 F. 3d 11, 18 n. 5 (1st Cir. 2005) (same); *Sanders v. Robert Bosch Corp.*, 38 F. 3d 736, 740 (4th Cir. 1994) (same); *George v. Carusone*, 849 F. Supp. 159, 163 (D. Conn. 1994) (same); *see also Awbrey v. Great Atlantic & Pacific Tea Co.*,

Here, by contrast, plaintiffs repeatedly allege that AT&T is conducting massive, wholesale surveillance of ordinary customers, including themselves, and AT&T does not even attempt to argue that those who actually *are* illegally surveilled do not have standing. While AT&T neither confirms nor denies the allegations, whether plaintiffs will ultimately be able to prove their claims is not at issue in this motion. *Nami v. Fauver*, 82 F.3d 63, 65 (3d Cir. 1996); *see also Lujan*, 504 U.S. at 566 (allegation of injury may be sufficient to survive a motion to dismiss, even if, on a motion for summary judgment, the facts do not exist to support the allegation); *Simon*, 426 U.S. at 45 n.25 (same).[9]

At its core, the Complaint alleges that AT&T is, as a factual matter, subjecting plaintiffs and millions of other innocent Americans to illegal surveillance and disclosure of private records. This is not a complaint on behalf of members of an organization who might be surveilled as possible terrorists; nor is it a complaint by concerned citizens based solely on their desire to change government policy, where standing is predicated on a right to require that the Government be administered according to law. *Cf. Nevada v. Burford*, 918 F.2d 854, 856-57 (9th Cir. 1990) ("An asserted right to have the Government act in accordance with law is not sufficient, *standing alone*, to confer jurisdiction on a federal court." (citations omitted) (emphasis added)).

Rather, the named plaintiffs and the class they represent have alleged that AT&T has intercepted and disclosed their private communications and records. The fact that the class consists of millions of AT&T customers does not turn this case into an unjusticiable generalized grievance.

---

505 F.Supp. 604, 606-607 (N.D. Ga. 1980) (allegations of continued, indiscriminate wiretapping sufficient to survive motion for summary judgment without evidence of specific phone calls tapped or listened to). Similarly, the statutes plainly prohibit AT&T from "knowingly divulging to any person or entity" the contents of plaintiffs' communications or records pertaining to them, without reference to what that person or entity eventually does with the disclosed material. 18 U.S.C. § 2702(a).

[9] For this reason, AT&T's citation to *Halkin v. Helms*, 690 F.2d 977 (D.C. Cir. 1982), is unpersuasive. "In the present case, there can be little doubt that the complaint alleged facts – interception of plaintiffs' private communications – which if proved would constitute an injury in fact, permitting plaintiffs to go forward in an effort to prove the truth of those allegations and any consequent liability of the defendants." *Id*. at 999. Rather, the court dismissed for lack of standing in that case because it had already ruled that the facts necessary to prove those allegations were privileged state secrets, an issue addressed in a separate motion. *See* Plaintiffs' Opposition to Gov't's Motion to Dismiss ("Opp. To Gov't Mot.") (to be filed June 8).

Sierra Club v. Morton, 405 U.S. 727, 734 (1972) ("[T]he fact that particular environmental interests are shared by the many rather than the few does not make them less deserving of legal protection through the judicial process."); *Common Cause v. Dep't of Energy*, 702 F.2d 245, 251 (D.C.Cir. 1983) ("[T]he widespread character of an alleged injury does not demean the standing of those who are in fact injured.").

B. Plaintiffs' Claims Are Not Subject To Dismissal On Grounds Of Statutory Immunity, or for Failure to Allege Absence of Such Immunity.

AT&T wrongly argues that plaintiffs have failed to plead the absence of "absolute immunity" under 18 U.S.C. § 2511(2)(a)(ii) (the "law enforcement assistance exception"), which authorizes service providers such as AT&T to assist in lawful surveillance. Neither the applicable notice pleading standards, Congress' intent, nor the plain language and structure of the statute creates such a pleading burden on plaintiffs. To the contrary, it is AT&T's burden to plead and prove its affirmative defenses, including one based on the argument that its conduct was lawfully authorized and undertaken in good faith. Nonetheless, even if plaintiffs do carry such a burden, the allegations in the Complaint meet it. Finally, regardless of burden, AT&T's conduct is wholly unlawful, going far beyond the bounds of Title III or FISA, and is therefore neither authorized nor immunized.

1. Plaintiffs Do Not Bear the Burden of Pleading the Absence of Lawful Authorization for AT&T's Conduct.

"FRCP 8(a), which states that a plaintiff's pleadings must contain 'a short and plain statement of the claim showing that the pleader is entitled to relief,' provides the standard for judging whether such a cognizable claim exists. . . . This standard is a liberal one that does not require a plaintiff to set forth all the factual details of the claim; rather, all that the standard requires is that a plaintiff give the defendant fair notice of the claim and the grounds for making that claim." *Brennan v. Concord EFS, Inc.*, 369 F.Supp.2d 1127 (N.D.Cal. 2005) (citing *Lee v. City of Los Angeles*, 250 F.3d 668, 679 (9th Cir. 2001); *Leatherman v. Tarrant County Narcotics Intell & Coordination Unit*, 507 U.S. 163 (1993)). Plaintiffs here meet the liberal notice pleading standard. Tellingly, AT&T makes no claim that it has not received fair notice of plaintiffs' claims.

The Supreme Court has repeatedly rejected efforts to impose "heightened pleading" standards in cases like this one in which no statute or rule expressly dictates. In *Swierkiewicz v. Sorema N.A.*, 534 U.S. 506 (2002), the Court held:

> Rule 8(a)'s simplified pleading standard applies to all civil actions, with limited exceptions. Rule 9(b), for example, provides for greater particularity in all averments of fraud or mistake. This Court, however, has declined to extend such exceptions to other contexts…. Thus, complaints in these cases, as in most others, must satisfy only the simple requirements of Rule 8(a).

534 U.S. at 513; *Porter v. Jones*, 319 F.3d 483, 495 (9th Cir. 2003) (applying *Sorema*; "we are to follow those pleading rules established in the Federal Rules of Civil Procedure and by statute, and . . . we are not to establish our own.").

Despite the established rule that heightened pleading requirements are improper except where expressly instructed by Congress,[10] and the plain lack of any express instructions from Congress in the statutes at issue, AT&T attempts to conjure up technical pleading requirements based on a partial reading of the legislative history. But where the statute's language is plain, no resort to legislative history is necessary. *Dep't of Hous. & Urban Dev. v. Rucker*, 535 U.S. 125, 132 (2002) ("[R]eference to legislative history is inappropriate when the text of the statute is unambiguous.").

However, even if the court were to consider the legislative history presented by AT&T, it is unpersuasive. The specific pleading requirements contemplated in the Senate Report for the Electronic Communications Privacy Act of 1986 ("ECPA"), 18 U.S.C. §§ 2701 *et seq.*, which AT&T cites, are wholly unreflected in the statute itself, and are also absent from the House's discussion of the same amendments to 18 U.S.C. § 2520. *See* H.R. Rep. No. 99-647, at 50 (1986).

---

[10] Congress knows how to use specific language to indicate technical pleading requirements, such as in cases involving securities fraud:

> *[T]he complaint shall specify* each statement alleged to have been misleading, the reason or reasons why the statement is misleading, and, if an allegation regarding the statement or omission is made on information and belief, *the complaint shall state with particularity* all facts on which that belief is formed…. *[T]he complaint shall*, with respect to each act or omission alleged to violate this chapter, *state with particularity* facts giving rise to a strong inference that the defendant acted with the required state of mind.

15 U.S.C. § 78u-4(b) (emphasis added). The statutes at issue here contain no such express requirements.

Both the House and the Senate Reports, however, do include language indicating that in order to obtain dismissal, a provider such as AT&T has the burden of showing the existence of a court order or other lawful authorization, and of showing that it acted in accord with that authorization in good faith:

> The term "good faith" as used in this section includes the receipt of a facially valid court order. Thus, the fact that the provider of electronic communication service also has received such a court order, means the provider would be entitled to a dismissal of a civil course of action *upon a showing that such provider acted within the scope of the court order*.

Id. (emphasis added)*; see also* S. Rep. No. 99-541, at 27 (1986), as reprinted in 1986 U.S.C.C.A.N. 3555, 3581 (using nearly identical language). Thus, even considering the legislative history, AT&T's argument that Congress somehow meant to infer a heightened pleading standard even while it did not specify one in the text must fail. Rather, it is AT&T's burden to affirmatively plead the lawfulness of its conduct.[11]

2. Lawful Authorization Is an Affirmative Defense for AT&T, not Plaintiffs, to Plead and Prove.

AT&T has the burden of affirmatively showing that its conduct was lawfully authorized, pursuant to the well-established principle of statutory construction holding that the party seeking the benefit of an exception to a statutory prohibition bears the burden of proof. *See U.S. v. First City Nat'l. Bank of Houston*, 386 U.S. 361, 366 (1967). Consistent with this rule, the exceptions to Title III, which are grouped together in subsection 18 U.S.C. § 2511(2), have been consistently characterized by courts as affirmative defenses. *See, e.g., Doe v. Smith*, 429 F.3d 706 (7th Cir.

---

[11] Lacking sufficient support for express pleading requirements in the statutes or their legislative history, AT&T cites two non-germane cases, *Williams v. Paulos*, 11 F.3d 271 (1st Cir. 1993), and *Thompson v. Dulaney*, 970 F.2d 744 (10th Cir. 1992). These cases lend no support for AT&T's argument, and in fact support the plaintiffs' position. These cases focus on the "use" and "disclosure" prohibitions under Title III, §§ 2511(1)(c) and 2511(1)(d), which are violated only when illegally intercepted communications are used or disclosed with knowledge of the illegal interception. 18 U.S.C. §§ 2511(1)(c), (1)(d); *see Williams*, 11 F.3d at 284; *Thompson*, 970 F.2d at 749. These cases stand only for the proposition that the plaintiff bears the burden of proving that the defendant knew of the illegality, and do not address the burden of pleading. *See Williams*, 11 F.3d at 284; *Thompson*, 970 F.2d at 749. Rather, *Williams* supports plaintiffs' contention that statutory exceptions need not be raised in the complaint but rather must be raised by AT&T, by holding that a plaintiff's burden of proof "includes a showing that any statutory exceptions *asserted by a defendant*, do not, in fact, apply." *Williams*, 11 F.3d at 284 (emphasis added).

2005) (reversing dismissal for failure to state a claim of wiretap lawsuit because plaintiff met notice pleading standard and was not required to "anticipate or attempt to defuse potential defenses" such as consent, § 2511(2)(d), in the complaint); *Blufome v. Pharmatrak, Inc. (In re Pharmatrak, Inc.)*, 329 F.3d 9, 19 (1st Cir. 2003) (burden of showing consent under § 2511(2)(d) is on the party seeking the benefit of the exception); *U.S. v. Jones*, 839 F.2d 1041, 1050 (5th Cir. 1988) (in criminal case, burden is on government to show consent under color of law under § 2511(2)(c) in order to avoid suppression of intercepted communications); *U.S. v. Harvey*, 540 F.2d 1345, 1352 n.9 (8th Cir. 1976) (in criminal case, burden is on government to demonstrate applicability of provider exception under § 2511(2)(a)(i) in order to avoid suppression). As with these other exceptions, it is AT&T's burden to affirmatively plead facts showing that it is entitled to benefit from the law enforcement assistance exception in § 2511(2)(a)(ii).

Placing the burden of pleading the absence of such exceptions on plaintiffs would further contradict the overall structure and intent of the relevant statutes. Title III contains more than a dozen statutory exceptions, many with subparts and exceptions to exceptions.[12] ECPA, upon which plaintiffs also rely, is similarly constructed.[13] Congress gave no indication that it intended these two statutes to create a maze of complex pleading demands that plaintiffs must negotiate or face the loss of their claims. To the contrary, it is much more logical and consistent for Congress to have intended defendants, who are in the possession of the relevant facts, to choose the appropriate defenses to plead in each particularized case. *Cf. Pharmatrak*, 329 F.3d at 19 (party asserting the consent exception is likelier to possess evidence of consent).

AT&T's argument otherwise suggests that Congress "hide[s] elephants in mouseholes." *Whitman v. Am. Trucking Ass'n*, 531 U.S. 457, 468 (2001). For if every plaintiff subject to surveillance were required to plead the non-existence of valid authorization under 18 U.S.C.

---

[12] *See, e.g.*, 18 U.S.C. §§ 2511(2)(a)(i) (provider protection); 2511(2)(a)(ii) (law enforcement and intelligence assistance); 2511(2)(b) (FCC monitoring); 2511(2)(c) (consent under color of law); 2511(2)(d) (consent not under color of law); 2511(2)(e) (FISA-related); 2511(2)(g)(i) (readily accessible to the general public); 2511(2)(g)(ii)(III) (intercepting radio communications in the amateur, CB, and GMRS spectrum bands).

[13] *See* 18 U.S.C. §§ 2702(b) (listing eight different exceptions for disclosure of communications) and 2702(c) (six for disclosure of customer records).

§ 2511(2)(a)(ii), even though the fact of such authorization cannot be obtained without "legal process," *id.*, meritorious cases would risk being dismissed prematurely before the factual question of authorization could be resolved through discovery. *See* MTD 10-11 (arguing that plaintiffs could never allege facts sufficient to state a claim because such facts are "completely unavailable to plaintiffs.").

This Catch-22 posed by AT&T's argument is clearly contradicted by the statutes. Again, Title III allows disclosure of such facts "as required by legal process" such as discovery, *see* 18 U.S.C. § 2511(2)(a)(ii), and to the extent the government objects that such disclosures would harm national security, it can invoke the procedures of 50 U.S.C. §§ 1806(f) and 1845(f), which allow *ex parte*, *in camera* inspection by the court and disclosure to plaintiffs as necessary to assess the surveillance's legality. *Id.* [14] It cannot be that Congress contemplated discovery of such facts under those provisions, yet intended for cases seeking such discovery to be dismissed at the pleading stage. Such a construction is contrary to Congress' clear intent to provide specific civil causes of action for those aggrieved by unlawful surveillance, whether conducted by the government or private parties, and even when conducted for foreign intelligence purposes. *See, e.g.*, 18 U.S.C. § 2520 (for violation of Title III), 50 U.S.C. § 1810 (for violation of FISA), 18 U.S.C. § 2707 (for violation of ECPA), and 18 U.S.C. § 2712 (for violations of Title III, FISA or ECPA by the United States). Furthermore, demanding that plaintiffs plead particular facts regarding a certification that may or may not exist is unnecessary because "on a motion to dismiss we presume that general allegations embrace those specific facts that are necessary to support the claim." *Nat'l Org. for Women v. Scheidler*, 510 U.S. 249, 256 (1994).

3. Even if Plaintiffs Did Bear the Burden to Plead Lack of Lawful Authorization, They Have Met That Burden.

Even assuming *arguendo* that AT&T is correct, and plaintiffs were required to plead in the

[14] These statutes specifically authorize the court to consider information that the government contends may harm national security. Therefore, AT&T's attempt to analogize them to the common-law state secrets privilege and argue that they were intended to "preclude judicial inquiry," MTD 9-10, is completely unavailing. For further discussion, see Opp. to Gov't Mot.

particular manner suggested in the partial legislative history it cites, plaintiffs have done so. According to the Senate Report cited by AT&T, "The complaint must allege that a wire or electronic communications service provider . . . acted without a facially valid court order or certification," "acted beyond the scope of a court order or certification," **or** "acted on bad faith;" "[a]cting in bad faith would include failing to read the order or collusion." S. Rep. No. 99-541, at 26 (1986), as reprinted in 1986 U.S.C.C.A.N. 3555, 3580.[15] While even under AT&T's view, plaintiffs need only allege one of these options, plaintiffs have already alleged all of them.

Plaintiffs have alleged actions in excess or in absence of any valid court order or certification by alleging that AT&T acted without "lawful authorization."[16] Complaint ¶ 81. Plaintiffs have also alleged AT&T acted in bad faith, because plaintiffs allege more than "simply bad judgment or negligence," but rather the "conscious doing of wrong because of dishonest purpose or moral obliquity." *See Theofel v. Farey-Jones*, 359 F.3d 1066, 1074 n.2 (9th Cir. 2004), *cert. denied*, 543 U.S. 813 (2004), *quoting Black's Law Dictionary* 139 (6th ed. 1990) (defining bad faith). In particular, plaintiffs allege that AT&T's wholly unauthorized collaboration with the government was undertaken "intentionally, with deliberate indifference, or with reckless disregard of Plaintiffs' and class members' constitutional rights," Complaint ¶ 87, "willful[ly] and for purposes of direct or indirect commercial advantage or private financial gain." *Id*. at ¶ 114; *see also id.* at ¶¶ 29-30, noting AT&T's reliance on the federal government as a major client.

AT&T's alleged misconduct, plaintiffs further plead, was the result of an "illegal collaboration" between it and the government, Complaint ¶ 8, whereby AT&T committed the complained of acts of interception and disclosure at the government's "instigat[ion]" or "direct[ion]," or with its "tacit[ ] approv[al]," *id.* at ¶ 82, but "without judicial or other lawful

---

[15] The legislative history that AT&T cites as supporting dismissal belies any notion of an "absolute" statutory immunity, since the Senate Report language plainly contemplates civil suits even in the presence of a certification or court order where the communications provider acted beyond its scope or in bad faith. *Id.*

[16] *Cf. Bivens v. Six Unknown Named Agents*, 403 U.S. 388 (1971) ("Petitioner's complaint does not explicitly state that the agents had no probable cause for his arrest, but it does allege that the arrest was 'done unlawfully, unreasonably and contrary to law,'" *id*. at 390 n. 1; "fairly read, it alleges as well that the arrest was made without probable cause." *Id*. at 389).

authorization." *id.* at ¶ 81. These allegations clearly plead "collusion" between AT&T and the government, i.e., "an agreement between two or more persons…to obtain an object forbidden by law," *Black's Law Dictionary* 264 (6th ed. 1990); the forbidden object, of course, is surveillance of plaintiffs' communications outside of the procedures of FISA and Title III, which are the exclusive means by which such surveillance may be conducted.

4. No Amount of Government Authorization Can Immunize AT&T from Liability for the Illegal Surveillance Activities Alleged in the Complaint.

Just as "the overriding principle in both *Berger* and *Katz*," the Supreme Court's primary precedents on wiretapping, "was the necessity for judicial control over electronic surveillance and a neutral predetermination of the scope of the search," *Kilgore v. Mitchell*, 623 F.2d 631, 635 (9th Cir. 1980), so were the statutes designed to ensure judicial control over wiretapping. *See* S. Rep. No. 90-1097 (1968), as reprinted in 1968 U.S.C.C.A.N. 2122, 2113 (Title III "conforms to the constitutional standards set out" in *Berger* and *Katz*); S. Rep. No. 95-604(I) at 6 (1978), as reprinted in 1978 U.S.C.C.A.N. 2904, 3908 (FISA meant to "spell out that the executive cannot engage in electronic surveillance within the United States without a prior judicial warrant.").[17]

Because of the overriding principle that the Fourth Amendment mandates judicial control over electronic surveillance, the instances under Title III and its sister statute FISA in which the Executive can initiate or continue surveillance without prior judicial approval are strictly cabined to four situations. *See* 50 U.S.C. § 1805(f) (allowing emergency FISA surveillance so long as court order obtained within 72 hours); 18 U.S.C. § 2518(7) (allowing emergency Title III surveillance so

[17] The counter-argument to AT&T's proposition that FISA does not reach any surveillance by the NSA, MTD at 12 n. 8, is already within the legislative history it cites: 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." S. Rep. No. 95-604(II) at 64 (1978), as reprinted in 1978 U.S.C.C.A.N. 3904, 3965 (emphasis added). FISA's definition of "electronic surveillance" plainly includes any domestic acquisition, *see* 50 U.S.C. § 1801(f)(2) (includes "the acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire communication to or from a person in the United States… if such acquisition occurs in the United States"), as well as any international acquisition targeted at Americans. *See* 50 U.S.C. § 1801(f)(1) (includes "the acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire or radio communication sent by or intended to be received by a particular, known United States person who is in the United States," regardless of location).

long as application for court order made within 48 hours); 50 U.S.C. § 1802 (allowing warrantless FISA surveillance of up to one year, only where solely directed at foreign powers and where there is no substantial likelihood of acquiring communications of U.S. persons, and requiring that any certifications upon which surveillance is based be immediately transmitted to the FISA court); 50 U.S.C. § 1811 (allowing warrantless FISA surveillance fifteen days following declaration of war). As the procedures of Title III and FISA are the "exclusive means" by which domestic interceptions and electronic surveillance may be conducted, they are the *only* situations allowing warrantless surveillance, and none of them is at all analogous to the ongoing warrantless dragnet surveillance alleged here.

In this Circuit, the requirements of Title III, which "were designed to protect the general public from abuse of the awesome power of electronic surveillance," *U.S. v. King*, 478 F.2d 494, 505 (9th Cir. 1973), "are not to be loosely interpreted," *id. at 503*.[18] When Congress enacted Title III, it intended to "make doubly sure that the statutory authority [for wiretaps] be used with restraint and only where the circumstances warrant the surreptitious interception of wire and oral communications." *U.S. v. Giordano*, 416 U.S. 505, 515 (1974). Consequently, government agents "are not free to ask or direct [the phone company] to intercept *any* phone calls or disclose their contents, at least not without complying with the judicial authorization provisions of the Wiretap Act," *McClelland v. McGrath*, 31 F.Supp.2d 616, 619 (N.D. Ill. 1998), and "all wire tapping by the telephone company is subject to close scrutiny by the courts. . . ." *U.S. v. Goldstein*, 532 F.2d 1305, 1311 (9th Cir. 1976).

AT&T argues that if it has "authorization" from the government, it may avoid liability for plain violations of the statutes, since "communications carriers authorized to assist the government

---

[18] The *King* court further warned:

> Concerns for the evils of crime is increasing in the United States, and not without justification. However, in such times it is especially important that the law not be bent in the name of expediency, especially not by the highest law enforcement official in the land.

478 F.2d at 505 (finding that Attorney General certification authorizing interceptions failed to meet formal requirements of Title III).

in foreign intelligence surveillance" are completely immune to liability. MTD at 6. Yet AT&T's use of the word "authority" is completely untethered from the statutory language, and Title III does not include such broad language. Instead, it only allows communications carriers to provide information, facilities, or technical assistance for interceptions and electronic surveillance to "persons authorized by law" to conduct such surveillance, and only when provided with a signed court order or a certification by the Attorney General or other specified persons that "no warrant or court order is required by law" and "that all statutory requirements have been met." 18 U.S.C. § 2511(2)(a)(ii). As Title III and FISA's statutory requirements are the "exclusive means" by which such surveillance may occur domestically, *see* 18 U.S.C. § 2511(2)(f), Section 2511(2)(a)(ii) only authorizes AT&T to assist with surveillance done in accord with court orders and certifications that are issued within the bounds of those statutes.[19] To the extent AT&T is conducting surveillance based on a certification that clearly goes beyond these bounds, its only resort is to plead and eventually prove the affirmative defense that it was acting in good faith. *See* 18 U.S.C. § 2520(d) (good faith defense to civil suit for illegal wiretapping); 18 U.S.C. § 2707(e) (same for violations of ECPA).

C. Plaintiffs' Claims Are Not Subject to Dismissal on Grounds of Absolute or Qualified Immunity.

The doctrines of absolute and qualified immunity provide defenses to damages liability for individual government officers who act in violation of constitutional or federal statutory law. *Nixon v. Fitzgerald*, 457 U.S. 731, 744-50 (1982); *Harlow v. Fitzgerald*, 457 U.S. 800, 807 (1982). While absolute immunity hews closely to its historical common-law origins, *Mitchell v. Forsyth*, 472 U.S. 511, 521 (1985), qualified immunity has undergone significant evolution and did not assume its

---

[19] Moreover, even assuming Section 2511(2)(a)(ii) could immunize AT&T against plaintiffs' statutory claims, it still would not warrant dismissal of their constitutional claims. *See Webster v. Doe*, 486 U.S. 592, 603 (1988) ("[W]here Congress intends to preclude judicial review of constitutional claims its intent to do so must be clear."); *cf. LaGuerre v. Reno*, 164 F.3d 1035, 1038-40 (7th Cir. 1998) (holding, despite statutory language directing that deportation orders "shall not be subject to review by any court," that "[t]he presumption that executive resolutions of constitutional issues are judicially reviewable . . . urges us to read into [that language] an exception that will allow the review of such issues.").

present form until *Harlow*. *Wyatt v. Cole*, 504 U.S. 158, 166 (1992) ("*Harlow* 'completely reformulated qualified immunity along principles not at all embodied in the common law'"). For the multiple independent reasons explained below, neither doctrine is a basis for dismissing plaintiffs' claims.

1. Neither Absolute Nor Qualified Immunity Bars the Injunctive and Other Equitable Relief Plaintiffs Seek on Each of Their Claims.

All of plaintiffs' claims seek injunctive and other equitable relief against defendants. *See* Complaint, Prayer for Relief. For their constitutional claims, Claim I, plaintiffs seek only declaratory and injunctive relief, not damages. Claims II through VI seek statutory damages as well as equitable relief, and Claim VII seeks only equitable relief.

Both absolute and qualified immunity are immunities to *damages* liability; neither affords immunity to claims for injunctive or other equitable relief. *Pulliam v. Allen*, 466 U.S. 522, 541-543 (1984) ("[Absolute] judicial immunity is not a bar to prospective injunctive relief against a judicial officer acting in her judicial capacity."); *Presbyterian Church v. U.S.*, 870 F.2d at 527 ("Qualified immunity is an affirmative defense to damage liability; it does not bar actions for declaratory or injunctive relief."); *American Fire, Theft & Collision Managers, Inc. v. Gillespie*, 932 F.2d 816, 818 (9th Cir. 1991) (same). It has long been the rule that illegal acts are enjoinable even when ultimately directed by government officers. *Youngstown Sheet & Tube Co. v. Sawyer*, 343 U.S. 579, 584 (1952) (enjoining Secretary of Commerce from obeying unconstitutional presidential order). "[I]n case of an injury threatened by his illegal action, the officer cannot claim immunity from injunction process. . . . [¶] The complainant did not ask the court to interfere with the official discretion of the Secretary of War, but challenged his authority to do the things of which complaint was made. The suit rests upon the charge of abuse of power, and its merits must be determined accordingly . . . ." *Philadelphia Co. v. Stimson*, 223 U.S. 605, 619-620 (1912) (citations omitted).

Because each of plaintiffs' claims seek injunctive relief and some seek other equitable relief as well, none of plaintiffs' claims can be dismissed on grounds of absolute or qualified immunity. At most, these immunities, if applicable to AT&T, would provide a defense only to damages liability; for the reasons we explain next, however, AT&T is entitled to neither absolute nor

qualified immunity and is subject to damages liability as well as equitable relief.

2. AT&T Is Not One of the Select Few Essential Government Actors Entitled to Absolute Immunity.

AT&T has no absolute immunity to damages liability for its participation in constitutional and federal statutory violations. "Our decisions have recognized immunity defenses of two kinds. For officials whose special functions or constitutional status requires complete protection from suit, we have recognized the defense of 'absolute immunity.' . . . [¶] For executive officers in general, however, our cases make plain that qualified immunity represents the norm." *Harlow*, 457 U.S. at 807. Accordingly, the Supreme Court has recognized absolute immunity only for a select few categories of government actors whose function in our system of government inescapably demands that they be accorded it: Presidents, legislators, judges, prosecutors, and witnesses. *Harlow*, 457 U.S. at 807; *Nixon*, 457 U.S. at 749 (President's absolute immunity is "a functionally mandated incident of the President's unique office"). "But this protection has extended no further than its justification would warrant." *Harlow*, 457 U.S. at 813. Cabinet officers, for example, do not possess absolute immunity; indeed, the Supreme Court has expressly held that "the Attorney General is not absolutely immune from suit for damages arising out of his allegedly unconstitutional conduct in performing his national security functions" in authorizing warrantless electronic surveillance. *Mitchell*, 472 U.S. at 520-21. Nor has absolute immunity ever been extended to private corporations.

AT&T is not entitled to absolute immunity because it is not an essential actor in our constitutional system of government like the President, a judge, or a legislator. It is a private, for-profit corporation selling services to consumers for the benefit of its shareholders. The functioning of the Republic does not demand that AT&T receive absolute immunity from liability for committing constitutional and statutory violations in the face of clearly established law to the contrary.

Moreover, AT&T cannot rely on the absolute immunity of others because government officers or private parties who participate in a constitutional or statutory violation with the President or another government actor possessing absolute immunity do not thereby derivatively

acquire absolute immunity themselves. *Harlow*, 457 U.S. at 810-11 (President's aides do not have derivative absolute immunity); *Dennis v. Sparks*, 449 U.S. 24 (1980) (private corporation and individuals who jointly participated with a judge in unconstitutional acts had no immunity even though judge had absolute immunity).

3. AT&T Has No "Absolute Common-Law Immunity."

"[I]n deciding whether officials performing a particular function are entitled to absolute immunity, we have generally looked for a historical or common-law basis for the immunity in question." *Mitchell*, 472 U.S. at 521. AT&T's hypothesized "absolute common-law immunity" (MTD at 13-15) for telecommunications providers relying on government authority is a chimera, for it has no historical or common-law basis. At common law, damages liability for illegal search and seizures was clearly established, even for wartime seizures made on authority of the President. More recently, the Ninth Circuit has rejected the notion that a telecommunications provider's cooperation with the government excuses liability for illegal surveillance.

a. The Common Law Imposes Damages Liability for Unlawful Searches and Seizures.

Historically, "[t]he Anglo-American tradition did not include a general theory of immunity from suit or from liability on the part of public officers." 2 HARPER & JAMES, *The Law of Torts*, § 29.8, at 1632 (1st ed., 1956). Thus, the common-law rule was that those who executed unlawful searches and seizures were liable in trespass. *The Apollon*, 22 U.S. (9 Wheat.) 362, 372-74 (1824) (Story, J.); *Gelston v. Hoyt*, 16 U.S. (3 Wheat.) 246, 310, 313-14, 320, 325 (1818) (Story, J.); *Murray v. Schooner Charming Betsy*, 6 U.S. (2 Cranch) 64, 116, 123-24 (1804) (Marshall, C.J.); *Entick v. Carrington*, 19 How. St. Tr. 1029 (C.P. 1765); *Wilkes v. Woods*, 19 How. St. Tr. 1153 (K.B. 1763).

The Supreme Court early on specifically rejected any immunity for persons who, at the direction of the executive, conduct searches and seizures during wartime that violate statutory limitations imposed by Congress. During the United States' first war, the undeclared naval war with France from 1798 to 1801, Congress authorized the President to direct the seizure of American ships that were traveling *to* French ports, but not those traveling *from* French ports.

President Adams, however, gave more expansive orders to the Navy that exceeded the searches and seizures authorized by Congress, and directed the seizure of American ships that were "bound to or from French ports." *Little v. Barreme,* 6 U.S. (2 Cranch) 170, 178 (1804). Adams did so for what we would call reasons of national security: "It was so obvious, that if only vessels sailing to a French port could be seized on the high seas, that the law would be very often evaded . . . ." *Id.*

Obeying the President's orders but acting contrary to the statutory limitations of Congress, the Navy frigate *Boston,* commanded by Captain Little, seized a ship coming *from* a French port it suspected with probable cause of being American and took the ship to Boston where it was libeled. The ship was adjudicated a neutral, and damages for its unlawful seizure and detention were imposed on Captain Little, a naval officer acting in a war zone at the direction of the Commander in Chief.

Writing for a unanimous Court, Chief Justice Marshall explained thus the Court's denial of immunity to Captain Little notwithstanding the Captain's good-faith obedience to his orders, and in doing so reviewed and rejected the same reliance-on-executive-authority argument that AT&T makes here:

> Is the officer who obeys [the instructions of the executive] liable for damages sustained by [the executive's] misconstruction of the act [of Congress], or will his orders excuse him? . . . [¶] I confess the first bias of my mind was . . . that though the instructions of the executive could not give a right, they might yet excuse from damages. . . . That implicit obedience which military men usually pay to the orders of their superiors, which indeed is indispensably necessary to every military system, appeared to me strongly to imply the principle that those orders, if not to perform a prohibited act, ought to justify the person whose general duty it is to obey them, and who is placed by the laws of his country in a situation which in general requires that he should obey them. I was strongly inclined to think that where, in consequence of orders from the legitimate authority, a vessel is seized with pure intention, the claim of the injured party for damages would be against that government from which the orders proceeded, and would be a proper subject for negotiation. But I have been convinced that I was mistaken, and . . . . that the instructions cannot change the nature of the transaction, or legalize an act which without those instructions would have been a plain trespass.

Little v. Barreme, 6 U.S. at 178-179; cited with approval in *Farid v. Smith,* 850 F.2d 917, 922 (2d Cir. 1988). The parallels are manifest: An Act of Congress imposing limitations on searches and seizures; an undeclared war; and an executive which orders searches and seizures beyond the scope of what Congress has authorized. Chief Justice Marshall's answer must be our own: a search or

seizure that is contrary to statute or Constitution, even when ordered by the President, gives rise to liability. Just as Captain Little was liable for his unlawful seizures, so must AT&T be.

b. The Ninth Circuit Has Held that Telecommunications Providers Are Liable for Assisting the Government in Illegal Surveillance.

This backdrop of common-law liability for unlawful seizures reveals that the "absolute common-law immunity" for telecommunications providers assisting the government that AT&T invokes is a fiction of its own creation. Moreover, in the context of Title III violations, the Ninth Circuit has examined and rejected the very argument made here by AT&T that a telecommunications provider's cooperation with the government immunizes it from liability. Instead, it has held that Congress intended the statutory good faith defense of 18 U.S.C. § 2520 to be the exclusive means by which a telecommunications provider may raise its cooperation with the government as a defense to liability:

> We appreciate [Nevada] Bell's concern that it may be held liable for cooperating with the police at the request of the Nevada state court. But the proper response to that concern is not to emasculate the statute. Congress appreciated this potential dilemma and established a defense for good faith reliance on a court order. It is upon such a defense that Bell must rely.

Jacobson v. Rose, 592 F.2d 515, 522 (9th Cir. 1978). In reaching this conclusion, the Ninth Circuit necessarily, and properly, rejected AT&T's argument that courts are free to ignore the statutory good faith defense and fashion their own unsupported, *ad hoc* defenses. Instead, it deferred to Congress, which has carefully crafted both the scope of liability and the statutory defenses available to telecommunications providers, and in doing so foreclosed any argument that courts can superimpose some form of "absolute common-law immunity" on top of Congress's statutory scheme.

The decision on which AT&T principally relies for its "absolute common-law immunity" argument, *Smith v. Nixon*, 606 F.2d 1183 (D.C. Cir. 1979), conflicts with the Ninth Circuit's decision in *Jacobson* and is not an immunity case. *Smith*, which addressed claims under the Constitution and 18 U.S.C. § 2511, does not purport to apply any rule of immunity from suit, much less an established "absolute common-law immunity." After reciting a sentence from the district court's opinion – "C&P's limited technical role in the surveillance as well as its reasonable

expectation of legality cannot give rise to liability for any statutory or constitutional violation," *Smith*, 606 F.2d at 1191 – the D.C. Circuit gave its two-sentence analysis: "We think this was the proper disposition. The telephone company did not initiate the surveillance, and it was assured by the highest Executive officials in this nation that the action was legal." *Id*.

The *Smith* court's conclusion that the telephone company was not liable is *ipse dixit*, devoid of any reasoned analysis or citation of supporting authority at all. At most, it suggests the court of appeals had in mind not immunity from suit, but some variety of good faith defense that had to be plead and proven. (The district court similarly described its holding as a conclusion that the telephone company had not acted wrongfully, not a conclusion that it was immune even if it had acted wrongfully: "There was no wrongdoing in this case by C&P." *Smith v. Nixon*, 449 F. Supp. 324, 326-27 (D.D.C. 1978).)

Moreover, unlike the Ninth Circuit in *Jacobson*, the *Smith* court failed to make any examination of the statutory language of Section 2520 that both creates civil liability for violations of Section 2511 and creates a good faith defense to civil liability, much less attempted to reconcile its conclusion of non-liability with this statutory language. The *Smith* court's conclusion is thus contrary to the Ninth Circuit's holding in *Jacobson* that the statutory good faith defense is exclusive.[20]

---

[20] There are plenty of other reasons why *Smith* does not control here. *Smith* predated, and thus does not address, the enactment of the civil liability provisions of 18 U.S.C. § 2707, 47 U.S.C. § 605, and 50 U.S.C. § 1810 on which plaintiffs rely. *Smith* also predated the Supreme Court's revolution in immunity law in *Harlow* (before that decision, qualified immunity was thought to involve the defendant's subjective good faith). In addition, the statutory good faith defense of 18 U.S.C. § 2520 has been amended significantly since the version applicable to *Smith*. *Smith* also stands in considerable tension with the D.C. Circuit's later conclusion in *Berry v. Funk*, discussed in the text, that there is no qualified immunity to Title III claims even for government officers.

The two other decisions AT&T relies on for its "absolute common-law immunity" also have no relevance here. *Fowler v. Southern Bell Tel. & Tel. Co.*, 343 F.2d 150 (5th Cir. 1965) presented only a *state* tort law claim for invasion of privacy, not any claim of constitutional or federal statutory violation. Thus, it does not involve absolute or qualified immunity for constitutional and federal statutory violations – the issue presented here – but an entirely different immunity doctrine, the official immunity of individual federal employees to *state* tort liability. 28 U.S.C. § 2679; *Westfall v. Erwin*, 484 U.S. 292, 295 (1988). This official immunity has never extended to claims like plaintiffs' for federal constitutional and statutory violations. 28 U.S.C. § 2679(b)(2); *Philadelphia Co.*, 223 U.S. at 619-620. Nor does it extend to claims for injunctive or other equitable relief, for it is limited to state law tort suits "for money damages." 28 U.S.C. § 2679(1); *Philadelphia Co.*, 223 U.S. at 619-620. Nor does it extend to private corporations like

Nor is AT&T correct that plaintiffs allege only that AT&T "merely allow[s] government surveillance to be conducted through the carrier's facilities." MTD at 15. To the contrary, plaintiffs allege that AT&T actively transmits the communications and call records of its customers to the government. Complaint ¶¶ 43-46, 52, 61, 81, 95, 103-105, 113, 121, 128. AT&T's minimalist version of its conduct is both inaccurate and no basis for a motion to dismiss.

4. No Qualified Immunity Defense Is Even Potentially Available to AT&T.

a. Qualified Immunity Is Available Only to Individuals, Not Corporations.

Independently, qualified immunity is not a potentially available defense here because qualified immunity is a defense to individual, not entity, liability. The Supreme Court has never extended qualified immunity to an entity, and for good reason. The purpose of qualified immunity is to shield *individual* officers from the disincentives and obstacles to effectively performing their duties that the potential for *personal* liability for damages might cause. These include "the distraction of officials from their governmental duties [by the demands of defending ongoing litigation], the inhibition of discretionary action [by the fear of damages liability], and deterrence of able people from public service." *Mitchell*, 472 U.S. at 526. The "most important" purpose of qualified immunity is to insure "vigorous," "principled and fearless decision-making" by *individuals*. *Richardson v. McKnight*, 521 U.S. 399, 408, 409 (1997).

None of these reasons supports extending qualified immunity to private corporations like AT&T. As the Supreme Court explained in *Owen v. Independence*, 445 U.S. 622, 653 n.37 (1980), when it denied qualified immunity to municipal corporations, "the justifications for immunizing

---

AT&T. *Adams v. United States*, 420 F.3d 1049, 1051, 1055 (9th Cir. 2005).

Craska v. New York Tel. Co., 239 F. Supp. 932 (N.D.N.Y. 1965) also does not avail AT&T. That case, which addressed only a claim under 47 U.S.C. § 605, was decided nearly 20 years before Congress in 1984 first created the express civil liability provision of section 605(e)(3). It has no bearing on the civil liability Congress created or whether Congress intended that telecommunications providers have absolute immunity to that liability. Nor does *Craska* conduct an immunity analysis or claim that it is recognizing an absolute immunity. Moreover, unlike here, in *Craska* it was the government, not the telephone company, which physically placed the wiretap on the plaintiff's phone line, intercepted the communications, and performed the acts that Section 605 prohibits of "divulg[ing]" and "publish[ing]" the communications.

officials from personal liability have little force when suit is brought against the governmental entity itself." To the contrary, making the entity fully liable creates strong institutional incentives for lawful conduct without dampening individual ardor:

> The knowledge that a municipality will be liable for all of its injurious conduct, whether committed in good faith or not, should create an incentive for officials who may harbor doubts about the lawfulness of their intended actions to err on the side of protecting citizens' constitutional rights. Furthermore, the threat that damages might be levied against the city may encourage those in a policymaking position to institute internal rules and programs designed to minimize the likelihood of unintentional infringements on constitutional rights.

Id. at 651-652.

These same considerations apply equally to private corporations. *See Owen*, 445 U.S. at 639 ("municipalities – like private corporations – were treated as natural persons for virtually all purposes of constitutional and statutory analysis"), 640 ("a municipality's tort liability in damages was identical to that of private corporations"). Because of the enormous power that governmental and corporate entities marshal and concentrate, bold and decisive action by individual decisionmakers who exercise control over an entity can cause the entity to wreak grave harm on others and on society at large if not channeled to lawful ends by adequate internal and external controls. The proper balance is struck when the individual receives qualified immunity or indemnity while the entity remains fully liable for the harms it causes, and is thereby encouraged to create an internal system of checks and balances that keeps the actions of its agents within the law.

b. Qualified Immunity Is Unavailable Because Telecommunications Providers Have No Common Law Immunity from Tort Actions and The Purposes of Qualified Immunity Do Not Extend to Them.

Even if AT&T were an individual rather than an entity, it still would not be entitled to qualified immunity. To determine whether qualified immunity is potentially available to a person, the first question is whether that person "was accorded immunity from tort actions at common law." *Tower v. Glover*, 467 U.S. 914, 920 (1984); *accord*, *Wyatt*, 504 U.S. at 164 (asking whether the "parties seeking immunity were shielded from tort liability"). Any such tort immunity must be "firmly rooted in the common law." *Wyatt*, 504 U.S. at 164; *accord*, *Richardson*, 521 U.S. at 404.

AT&T is unable to satisfy this prerequisite for qualified immunity because

telecommunications providers do not possess any firmly rooted immunity at common law from tort actions. To the contrary, there was a firmly rooted common-law tradition imposing liability on them for their torts, including for their malfeasance in handling communications entrusted to them.[21] *See, e.g.*, *Gonzales v. Southwestern Bell Tel. Co.*, 555 S.W.2d 219, 221 (Tex. App. 1977); *Le Crone v. Ohio Bell Tel. Co.*, 201 N.E.2d 533 (Ohio Ct. App. 1963) (wiretapping); *Critz v. Southern Bell Tel. & Tel. Co.*, 172 So. 510, 512 (Miss. 1937); *Western Union Tel. Co. v. Ramsey*, 88 S.W.2d 675, 677 (Ky. Ct. App. 1935); *Vinson v. Southern Bell Tel. & Tel. Co.*, 66 So. 100 (Ala. 1914); *Joshua L. Bailey & Co. v. Western Union Tel. Co.*, 76 A. 736, 741 (Pa. 1910); *McLeod v. Pacific States Tel. & Tel. Co.*, 94 P. 568, *on rhg.*, 95 P. 1009 (Or. 1908), *Southern Bell Tel. & Tel. Co. v. Earle*, 45 S.E. 319, 321 (Ga. 1903).

Nor do the purposes of qualified immunity support extending it to telecommunications providers. As explained previously, the most important purpose of qualified immunity – ensuring that fear of personal damages liability does not stop individual government officers from acting decisively – has no application to a multibillion-dollar private for-profit corporation like AT&T.

As the Supreme Court has noted:

> [T]he rationales mandating qualified immunity for public officials are not applicable to private parties. [¶] . . . [¶] . . . Although principles of equality and fairness may suggest, as respondents argue, that private citizens who rely unsuspectingly on state laws they did not create and may have no reason to believe are invalid should have some protection from liability, as do their government counterparts, such interests are not sufficiently similar to the traditional purposes of qualified immunity to justify such an expansion. Unlike school board members, or police officers, or Presidential aides, private parties hold no office requiring them to exercise discretion; nor are they principally concerned with enhancing the public good. Accordingly, extending *Harlow* qualified immunity to private parties would have no

---

[21] AT&T misapplies this test in two respects. First, it misconceives the relevant activity too narrowly in describing it as "cooperat[ing] with government officials conducting warrantless surveillance." MTD at 16. Here, the proper focus is on the activity of providing telecommunications services to consumers, just as in *Tower* the relevant activity was legal representation of criminal defendants, 467 U.S. at 921-22, and in *Richardson* the activity was "prison management activities," 521 U.S. at 407. Second, AT&T erroneously asserts that a single case, *Smith v. Nixon*, amounts to a firmly rooted tradition of common-law immunity to tort liability. As explained above, *Smith* is not an immunity case, conflicts with the Ninth Circuit's decision in *Jacobson*, and in any event is not evidence of a firmly rooted tradition of common-law tort immunity, as it is not a tort case at all, but a constitutional and statutory liability case. To look to a constitutional and statutory liability case like *Smith* to decide whether there is a preexisting tradition of common-law immunity to tort liability inverts the proper analysis.

> bearing on whether public officials are able to act forcefully and decisively in their jobs or on whether qualified applicants enter public service. Moreover, unlike with government officials performing discretionary functions, the public interest will not be unduly impaired if private individuals are required to proceed to trial to resolve their legal disputes. In short, the nexus between private parties and the historic purposes of qualified immunity is simply too attenuated to justify such an extension of our doctrine of immunity.

Wyatt, 504 U.S. at 168 (citations omitted); *accord*, *Richardson*, 521 U.S. at 412 (refusing qualified immunity to private prison guards); *Tower*, 467 U.S. at 922-23 (refusing immunity to public defenders, who are considered to be private persons for purposes of Section 1983; "[w]e do not have a license to establish immunities . . . in the interests of what we judge to be sound public policy.").

AT&T's argument that telecommunications providers will be reluctant to assist in government surveillance absent qualified immunity (MTD at 17) lacks merit. The government can compel by court order the assistance of telecommunications providers in electronic surveillance activities, and good faith reliance on that order provides them with a defense to liability. *See, e.g.*, 18 U.S.C. §§ 2518(4), 2520(d); *U.S. v. New York Tel. Co.*, 434 U.S. 159, 174-78 (1977); *Company v. U.S. (In re U.S.)*, 349 F.3d 1132, 1139 (9th Cir. 2003).

c. Qualified Immunity Does Not Apply to Plaintiffs' Statutory Claims.

Nor is there a qualified immunity defense available to plaintiffs' federal statutory claims. In each of those statutes, as explained above, Congress has carefully crafted the scope and limits of liability and has also created good faith defenses to liability. 18 U.S.C. §§ 2520(d), 2707(e); 47 U.S.C. § 605(e)(3)(C)(iii); 50 U.S.C. § 1809(b). There is no basis in these statutes for a court to imply qualified immunity on top of the carefully nuanced statutory scheme of liability and good faith defenses that Congress has created, and to do so would violate congressional intent.

As the D.C. Circuit has explained:

> the qualified immunity doctrine applied to constitutional torts and § 1983 actions has no application to [these] statutory claims. That is so because Title III itself provides a complete defense for "[a] good faith reliance on . . . a court warrant or order, a grand jury subpoena, a legislative authorization, or a statutory authorization." 18 U.S.C. § 2520(d) (1994). . . . When Congress itself provides for a defense to its own cause of action, it is hardly open to the federal court to graft common-law defenses on top of those Congress creates. *See City of Milwaukee v.*

> *Illinois*, 451 U.S. 304, 314 (1981) ("When Congress addresses a question previously governed by a decision rested on federal common law the need for such an unusual exercise of lawmaking by federal courts disappears."). This is particularly so when Congress provides for a good faith defense that is more limited than the qualified immunity good faith doctrine the judiciary has devised; Congress, it might be said, has "occupied the field."

Berry v. Funk, 146 F.3d 1003, 1013 (D.C. Cir. 1998).

This conclusion accords with the Ninth Circuit's holding in *Jacobson*, discussed above, that the statutory good faith defense of Section 2520 is the exclusive defense to liability under that statute.

The decisions to the contrary that AT&T relies on are not persuasive. The courts in *Tapley v. Collins*, 211 F.3d 1210 (11th Cir. 2000) and *Blake v. Wright*, 179 F.3d 1003 (6th Cir. 1999), superimposed qualified immunity on top of the good faith defense of 18 U.S.C. § 2520(d). For the reasons stated above, the better view, and the one compelled by *Jacobson*, is that Congress intended the explicit statutory defenses it created to be exclusive.

5. Qualified Immunity Is Unavailable for Plaintiffs' Claims Because They Are All Based on Clearly Established Law.

Finally, even if qualified immunity were a potentially available defense here, it would fail on these facts. AT&T misstates the two stages of qualified immunity analysis: the first question is whether "the facts alleged" show that the defendant has violated a constitutional or statutory right; the second is whether the right is "clearly established," i.e., whether "it would be clear to a reasonable officer that his conduct was unlawful in the situation he confronted." *Saucier v. Katz*, 533 U.S. 194, 201-202 (2001). (Contrary to AT&T, MTD at 18, this second inquiry has nothing to do with "bad faith." *Wyatt*, 504 U.S. at 165-66.) AT&T's argument that the Complaint does not allege a violation of plaintiffs' rights holds no water, because that argument is based on the "one-end foreign, one-end Al Qaeda-related" surveillance admitted by the government, rather than on the broader surveillance Program that plaintiffs allege.

Turning to the second inquiry, it would be clear to a reasonable telecommunications provider that massive suspicionless interception and disclosure of Internet messages and call records is unlawful. As explained at length in plaintiffs' preliminary injunction motion (Dkt. 30), it

has been clearly established since the Founding that the Fourth Amendment prohibits suspicionless general searches of the type and massive scale occurring here. *See, e.g.*, *Andresen v. Maryland*, 427 U.S. 463, 482 (1976); *Stanford v. Texas*, 379 U.S. 476, 481-86 (1965). In particular, "[i]t is now clear that [the warrant] requirement attaches to national security wiretaps that are not directed against foreign powers or suspected agents of foreign powers." *Halperin v. Kissinger*, 807 F.2d 180, 185 (D.C. Cir. 1986) (Scalia, Circuit Justice). The plaintiff class expressly excludes foreign powers and agents of foreign powers. Complaint ¶ 70.

It would also be clear to a reasonable telecommunications provider that the alleged interceptions and disclosures violate the statutory provisions asserted by plaintiffs. (Because statutes are typically much more explicit and detailed than the Constitution, the question of whether a statutory right is "clearly established" arises with much less frequency than in the case of constitutional rights.) With respect to plaintiffs' Communications Act claim, the Supreme Court held decades ago: "[T]he plain words of § 605 forbid anyone, unless authorized by the sender, to intercept a telephone message, and direct in equally clear language that 'no person' shall divulge or publish the message or its substance to '*any person*.' " *Nardone v. U.S.*, 302 U.S. 379, 382 (1937). ECPA's prohibitions on the unconsented disclosure of stored communications and records are equally plain: electronic communications service providers like AT&T "shall not knowingly divulge" such communications "to any person or entity," or such records "to any governmental entity," except as consistent with specific exceptions inapplicable here. *See* 18 U.S.C. §§ 2702 (general prohibition and exceptions), 2703 (procedures for disclosure to government). Finally, and as already discussed, Title III and FISA place clear limits on when communications providers may assist the government in conducting interceptions and electronic surveillance, limits that AT&T has far exceeded. *See* Section A.4, *supra*.

IV. CONCLUSION

For the foregoing reasons, AT&T's motion to dismiss should be denied. In the alternative, plaintiffs respectfully request leave to amend their complaint to address any deficiencies this Court finds therein.

DATED: June 6, 2006

ELECTRONIC FRONTIER FOUNDATION

By _____
Cindy A. Cohn, Esq. (SBN.145997)
Lee Tien, Esq. (SBN 148216)
Kurt Opsahl, Esq. (SBN 191303)
Kevin S. Bankston, Esq. (SBN 217026)
Corynne McSherry, Esq. (SBN 221504)
James S. Tyre, Esq. (SBN 083117)
454 Shotwell Street
San Francisco, CA 94110
Telephone: (415) 436-9333 x108
Facsimile: (415) 436-9993

ATTORNEYS FOR PLAINTIFFS

HELLER EHRMAN LLP
ROBERT D. FRAM
MICHAEL M. MARKMAN
ETHAN C. GLASS
SAMUEL F. ERNST
NICOLE ACTON-JONES
NATHANIEL SHAFROTH
ELENA DIMUZIO
333 Bush Street
San Francisco, CA 94104
Telephone: 415/772-6000
415-772-6268 (fax)

LERACH COUGHLIN STOIA GELLER RUDMAN & ROBBINS LLP
REED R. KATHREIN
JEFF D. FRIEDMAN
SHANA E. SCARLETT
MARIA V. MORRIS
100 Pine Street, Suite 2600
San Francisco, CA 94111
Telephone: 415/288-4545
415/288-4534 (fax)

TRABER & VOORHEES
BERT VOORHEES (137623)
bv@tvlegal.com
THERESA M. TRABER (116305)
tmt@tvlegal.com
128 North Fair Oaks Avenue, Suite 204
Pasadena, CA 91103
Telephone: 626/585-9611
626/ 577-7079 (fax)

LAW OFFICE OF RICHARD R. WIEBE
RICHARD R. WIEBE
425 California Street, Suite 2025
San Francisco, CA 94104
Telephone: 415/433-3200
415/433-6382 (fax)

LERACH COUGHLIN STOIA GELLER RUDMAN & ROBBINS LLP
ERIC ALAN ISAACSON
655 West Broadway, Suite 1900
San Diego, CA 92101
Telephone: 619/231-1058
619/231-7423 (fax)

CERTIFICATE OF SERVICE

I hereby certify that on June 6, 2006, I electronically filed the foregoing with the Clerk of the Court using the CM/ECF system which will send notification of such filing to the e-mail addresses denoted on the attached Electronic Mail Notice List, and I hereby certify that I have mailed the foregoing document or paper via the United States Postal Service to the following non-CM/ECF participants:

David W. Carpenter
Sidley Austin Brown & Wood LLP
Bank One Plaza
10 South Dearborn Street
Chicago, IL 60600

David L. Lawson
Sidley Austin Brown & Wood
172 Eye Street, N.W.
Washington, DC 20006

By /s/
Cindy A. Cohn, Esq. (SBN.145997)
ELECTRONIC FRONTIER FOUNDATION
454 Shotwell Street
San Francisco, CA 94110
Telephone: (415) 436-9333 x108
Facsimile: (415) 436-9993
cindy@eff.org