WILMER CUTLER PICKERING
HALE AND DORR LLP
John A. Rogovin (*pro hac vice*)
Randolph D. Moss (*pro hac vice*)
Samir C. Jain SBN 181572
Brian M. Boynton SBN 222193
Catherine M.A. Carroll (*pro hac vice*)
1875 Pennsylvania Avenue, N.W.
Washington, D.C. 20006
Telephone: (202) 663-6000
Fax: (202) 663-6363
Email: john.rogovin@wilmerhale.com

Randal S. Milch (*pro hac vice*)
Verizon Communications Inc.
One Verizon Way, VC 43E043
Basking Ridge, NJ 07920
Telephone: (908) 559-1752
Fax: (908) 696-2136

MUNGER, TOLLES & OLSON LLP
Henry Weissmann SBN 132418
Susan R. Szabo SBN 155315
Aimee A. Feinberg SBN 223309
355 South Grand Avenue, Suite 3500
Los Angeles, CA 90071-1560
Telephone: (213) 683-9100
Facsimile: (213) 687-3702
Email: Henry.Weissmann@mto.com

Attorneys for Verizon Communications Inc., Verizon Northwest Inc., Verizon Florida Inc., and MCI Communications Services, Inc.

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN FRANCISCO DIVISION

IN RE:

NATIONAL SECURITY AGENCY TELECOMMUNICATIONS RECORDS LITIGATION

This Document Relates To:

All Actions Against the MCI and Verizon Defendants in the Master MCI and Verizon Consolidated Complaint, Dkt. 125

MDL NO. 06-1791 VRW

REPLY MEMORANDUM IN SUPPORT OF VERIZON'S MOTION TO DISMISS PLAINTIFFS' MASTER CONSOLIDATED COMPLAINT

Hearing Date: August 30, 2007
Time: 2:00 p.m.
Courtroom: 6 (17th floor)
Judge: Hon. Vaughn R. Walker

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page

FEDERAL CASES

TABLE OF AUTHORITIES
(continued)

Page

TABLE OF AUTHORITIES
(continued)

Page

TABLE OF AUTHORITIES
(continued)

Page

TABLE OF AUTHORITIES
(continued)

Page

STATE CASES

FEDERAL STATUTES

TABLE OF AUTHORITIES
(continued)

Page

STATE STATUTES

LEGISLATIVE HISTORY

FEDERAL RULES AND REGULATIONS

TREATISES

OTHER AUTHORITIES

I. INTRODUCTION

Plaintiffs' Opposition ("Opp.") makes a number of concessions that substantially narrow the issues and lead inexorably to the conclusion that defendants' motion must be granted.

Plaintiffs do not contest that ECPA, Title III, and 47 U.S.C. § 605 cannot be construed to apply to the facts alleged absent a "clear statement" of intent to do so. This tacit concession alone requires dismissal of the claims based on these statutes because their language and history contain no indication that Congress even considered using these statutes to constrain the President's constitutional authority to collect intelligence to defend the nation against terrorist attacks—in sharp contrast to FISA, where Congress expressly and extensively considered whether, and to what extent, to limit the President's ability to collect national security intelligence.

Plaintiffs also do not dispute that the alleged communication of call records would be speech and that applying ECPA to such alleged speech triggers First Amendment review. Even under the intermediate scrutiny and balancing tests that plaintiffs advocate, let alone under the strict scrutiny standard that properly controls, applying ECPA to the unique circumstances alleged would violate the First Amendment. Plaintiffs similarly fail to contest that the First Amendment requires prompt disposition of the records claims. Defendants' Opening Brief ("OB") 26-27.

Plaintiffs also fail to respond meaningfully to defendants' showing that ECPA can be read to not apply to the facts alleged, and that it must be so read to avoid these constitutional issues. For example, while plaintiffs argue that the emergency and rights and property exceptions *could* be construed narrowly, they do not come close to showing that ECPA unambiguously forecloses the conclusion that the alleged communication of records to the government for the purpose of preventing terrorist attacks would fall within these exceptions, particularly given the considered judgment of the political branches that the threat of such attacks presents an ongoing emergency.

Finally, plaintiffs' opposition demonstrates that the state-secrets doctrine mandates immediate dismissal. Plaintiffs repeatedly insist that various arguments defendants have advanced cannot be resolved without resort to facts. We show that the allegations of the Complaint themselves establish that plaintiffs' claims fail as a matter of law. But even if the facts

plaintiffs say they need were relevant, the government's assertion of the state-secrets privilege would render them unavailable. According to plaintiffs, these are not issues that might arise at some future point in the litigation: plaintiffs have put them at issue now. It would be unfair to subject defendants to the continued threat of crippling liability when the government's assertion of the privilege prevents them from litigating facts that plaintiffs contend are dispositive.

Below, we first show that the records claims under ECPA must be dismissed. Next, we explain that the claims based on the alleged interception of call content are governed exclusively by FISA, and that the FISA claim must also be dismissed. Finally, we show that the other statutory and state-law claims fail, and that the bankruptcy discharge bars the claims against MCI.

II. ECPA DOES NOT APPLY TO THE ALLEGED COLLECTION OF RECORDS FOR NATIONAL SECURITY INTELLIGENCE PURPOSES

A. ECPA Lacks the Required Clear Statement

Plaintiffs do not contest that ECPA cannot be construed to apply to the facts alleged absent a "clear statement." OB 12-14; Opp. 16 & n.15. Because the President has independent authority under Article II to collect intelligence from private parties to defend the nation from attack, and because the Complaint alleges that records were collected for that purpose, applying ECPA in this unusual circumstance would constrain the President's constitutional powers. Principles of inter-branch comity and the requirement that courts avoid interpreting statutes to raise serious constitutional problems have led courts to insist that Congress express its intent to constrain the constitutional powers of another branch in clear and unmistakable terms. OB 13-14.

ECPA's prohibition on divulgence of records "to any governmental entity," 18 U.S.C. § 2702(a)(3), is not a clear statement. Opp. 14. On the contrary, the clear statement rule comes into play precisely when a statute contains such broad language. The whole point of the rule is that Congress may not have considered the possibility that a generally-worded prohibition would apply to the exercise of Presidential power, and therefore a clearer statement of intention to apply the prohibition to constrain the constitutional powers of a co-equal branch is required.

Franklin v. Massachusetts, 505 U.S. 788 (1992), is controlling. *Franklin* considered whether the Administrative Procedure Act ("APA") applies to the President. Like ECPA, the

APA uses broad language: it defines "agency" as "each authority of the Government of the United States" and specifically excepts Congress and the courts (but not the President). 5 U.S.C. § 701(b)(1). The Court held that the APA could not be read to apply to the President absent an "express statement," and that neither the APA's reference to "each authority" nor the iteration of exceptions other than the President constituted such a statement. *Franklin*, 505 U.S. at 800-01; *see also Pub. Citizen v. Dep't of Justice*, 491 U.S. 440, 455 (1989) (based on separation of powers concerns, statutory term "utilize" should be construed as not including use of ABA in evaluating judicial nominations even though statute read literally would sweep in such use); *United States v. Butenko*, 494 F.2d 593, 601 (3d Cir. 1974) (en banc) (47 U.S.C. § 605, prohibiting disclosure of intercepted communication to "any person," would not be construed to restrict President's conduct of foreign intelligence). Likewise, ECPA's broadly-worded prohibition on divulgence to "any governmental entity," combined with exceptions allowing divulgence in some situations, is not a clear statement of intent to constrain the President's constitutional powers. In this context, the issue is not whether a statute *expressly* "excepts" the President's exercise of constitutional powers, Opp. 14, but whether the statute *expressly applies* to that activity.

The contrast with FISA confirms that ECPA does not curtail the President's authority over national security intelligence. Before adopting FISA, Congress spent years debating its power to limit the President's constitutional authority. OB 15 & n.11. In FISA, Congress specifically confronted those constitutional issues, sought to implement a countervailing constitutional right under the Fourth Amendment, and stated that FISA's procedures would be the "exclusive means" of engaging in surveillance for national security. OB 15-16. ECPA lacks any of these indications of intent to constrain the President's constitutional powers. ECPA did not *sub silentio* grapple with the serious constitutional problems to which Congress devoted so much attention in FISA.

ECPA's structure also shows that it was not meant to constrain intelligence-gathering for national defense. For example, FISA permits warrantless surveillance for the first 15 days of a war, but ECPA has no similar exception. Had ECPA constrained the President's ability to collect records for national defense, it would have included a similar exception. OB 16. Likewise, ECPA's provisions allowing the government to compel production of records for mundane

purposes render implausible the suggestion that Congress meant to curtail the President's ability to collect records to protect the nation. *Id*. Plaintiffs' failure to respond to these points is telling.

The additional authority that 18 U.S.C. § 2709 gives the FBI to *compel* production of records is far from a clear statement of intent to constrain the President's constitutional authority to collect intelligence from voluntary sources. OB 17-18; Opp. 15. Just as the iteration of exceptions is not a clear statement of intent for a general prohibition to apply to the President, *Franklin*, 505 U.S. at 800-01, a grant of power in one situation is not a clear statement of intent to constrain the President's power in another situation. This conclusion is even more strongly required as to § 2709 for two reasons. First, whereas Congress stated that the procedures of ECPA, Title III, and FISA are the "exclusive means" by which the *content* of calls can be acquired, 18 U.S.C. § 2511(2)(f), it refrained from imposing a similar limit on the collection of *records*. Section 2709, and ECPA as a whole, are thus not the only means by which the President can lawfully obtain records for national security. OB 12, 18. Second, § 2709's legislative history shows that Congress intended to preserve voluntary arrangements and to preempt states from interfering with the FBI's ability to obtain records. "The new mandatory FBI authority for counterintelligence access to records *is in addition to, and leaves in place, existing non-mandatory arrangements for FBI access based on voluntary agreement of communications common carriers*." S. Rep. No. 99-307, at 19 (1986) (emphasis added); *see also* OB 17-18. This history refutes plaintiffs' assertion of a clear statement, for the Supreme Court has held that it is "imperative" to "consider indicators of congressional intent"—specifically, legislative history—before concluding that a federal statute restricts Article II power. *Pub. Citizen*, 491 U.S. at 455. Plaintiffs' suggestion that this legislative history be ignored, Opp. 16, not only misapprehends the law but also is a tacit admission that the history of § 2709's enactment is fatal to their argument.

The provision *in FISA* authorizing the FBI to obtain orders compelling production of records, 50 U.S.C. § 1861, *see* Opp. 16, is irrelevant in determining whether *ECPA* contains a clear statement. Because the authority granted to the FBI in § 2709 of ECPA cannot be construed as a clear statement of intent to constrain the President's power to collect records through voluntary arrangements, *a fortiori* a provision in *another statute* granting the FBI additional

authority likewise cannot be so construed. Also, requiring the President to rely solely on the FBI to gather national security intelligence would raise serious constitutional problems. OB 18 n.12. ECPA lacks a clear statement that Congress meant to test these constitutional limits.

The other statutes plaintiffs cite are inapposite. Opp. 15-16. ECPA section 107 does not prohibit any intelligence activities. Pub. L. No. 99-508, § 107(a), 100 Stat. 148 (1986). Plaintiffs say that 18 U.S.C. § 2511(2)(f) exempts the collection of international or foreign call records and therefore impliedly restricts the collection of domestic records. But under *Franklin*, a statement that statutory provisions do not apply in one situation is not a clear statement that they do apply in other situations involving the exercise of constitutional powers. Moreover, plaintiffs' characterization of the first clause of § 2511(2)(f) is wrong. The foreign intelligence information to which that clause refers is the "acquisition" of content through surveillance—i.e., information "from" communications. *Id*.; *see also* H.R. Rep. No. 95-1283, at 100 (1978) (describing § 2511(2)(f) as involving "surveillance"). Records fall outside this provision. They are information "pertaining to" a customer, 18 U.S.C. § 2702(a)(3), not information "from" communications. *See also infra* at 32 (discussing structure and purpose of § 2511(2)(f)).

B. The AUMF Provides Statutory Authority

If ECPA were construed to constrain the President's collection of records for national defense purposes, it would become necessary to determine whether the Authorization for Use of Military Force ("AUMF") gave the President such authority. Plaintiffs' claim that it does not elides a critical difference between FISA and ECPA. Unlike FISA, ECPA does not state that its procedures are the "exclusive means" for the government to obtain records. Thus, plaintiffs' claim that the AUMF did not authorize *surveillance* outside of *FISA's* procedures, Opp. 17, while incorrect, is beside the point as to ECPA.

ECPA states that "statutory authorization" to provide records can exist outside of ECPA. 18 U.S.C. §§ 2703(e), 2707(e). When a statutory prohibition is subject to an exception for actions taken pursuant to a later statute, and those actions are accepted incidents of war, the AUMF provides the requisite authorization. *Hamdi v. Rumsfeld*, 542 U.S. 507, 518 (2004) (plurality opinion); *id*. at 587 (Thomas, J., dissenting); *see also* OB 19. By contrast, in *Hamdan v.*

Rumsfeld, 126 S. Ct. 2749 (2006), the earlier statute provided authority for military tribunals only to the extent consistent with the law of war, and the AUMF did not impliedly repeal the earlier statute. *Id*. at 2775. The AUMF does not repeal ECPA; it gives the President the kind of authority that ECPA says may be supplied.

Plaintiffs concede that the "AUMF may authorize activities that are 'accepted incidents of war,'" Opp. 18 (citation omitted), and they do not dispute that gathering intelligence about the enemy, identifying enemy agents, and determining the enemy's plans are traditional warmaking activities, *see* OB 13, 19. Accordingly, the absence of "specific language" in the AUMF referencing the gathering of records "is of no moment." *Hamdi*, 542 U.S. at 519 (plurality opinion); *see also id*. at 587 (Thomas, J., dissenting). Plaintiffs further suggest that intelligence relating to a foreign enemy's activities cannot be gathered inside the U.S. Opp. 18. But the AUMF authorizes the President to take action to prevent future attacks "both at home and abroad." AUMF pmbl., § 2(a). In an armed conflict in which enemy operatives seek to insinuate themselves into this country to launch attacks, developing the capability to query data to detect such operatives, as plaintiffs allege, would be a traditional aspect of warmaking—particularly because the alleged activities would not implicate the Fourth Amendment. The historical record is clear that during armed conflicts Presidents have authorized the collection of intelligence inside the U.S. that could be relevant to the activities of foreign enemies. For example, in 1940, President Roosevelt directed warrantless surveillance within the U.S. of suspected spies and those engaged in "fifth column" activities. *See United States v. U.S. Dist. Ct.*, 444 F.2d 651, 669-70 (6th Cir. 1971) (reproducing FDR's memo), *aff'd*, 407 U.S. 297 (1972); *see also, e.g.*, Exec. Order No. 8985, 6 Fed. Reg. 6625 (Dec. 19, 1941) (authorizing censorship, and *a fortiori* interception, of all communications from U.S. to foreign countries); Exec. Order No. 2604 (Apr. 28, 1917) (similar order issued by President Wilson in World War I). Indeed, even in the *Cold* War, Presidents consistently authorized collection within the U.S. of intelligence that could relate to Soviet activities, including specifically call records, and that authority has never been doubted. *See* OB 17 (discussing legislative history of § 2709). The same would hold for the collection of records to track the activities of terrorists in the context of declared hostilities.

C. *Ashwander* and State-Secrets Compel This Result

Construing ECPA to restrict the President's ability to collect records for national security purposes would raise a serious constitutional problem. OB 17. Plaintiffs do not dispute that this constitutional problem triggers *Ashwander*; therefore, ECPA's emergency exception must be construed, if possible, to cover the activities alleged. Clearly, that exception can be so construed. OB 20-22. In addition, to determine if ECPA could constitutionally be applied to constrain the President would require evidence about the justifications for the alleged records program. The state-secrets privilege renders any such evidence unavailable. OB 22.

III. THE RECORDS CLAIMS SEEK TO IMPOSE LIABILITY FOR ALLEGED ACTIVITY PROTECTED BY THE FIRST AMENDMENT

Plaintiffs concede that the alleged divulgence of records would be speech and that restrictions on such alleged speech must pass muster under the First Amendment. Under established First Amendment doctrine, the application of ECPA to the facts alleged would be unconstitutional because the privacy interests plaintiffs assert are slight and cannot outweigh defendants' right to speak on a matter of public importance.

Punishing a private party for speaking is fundamentally different than restricting the *government's* actions. The Fourth Amendment limits the government's power. Congress can further limit government power (within constitutional boundaries) by specifying when the Executive can compel production of information held in private hands and how the Executive handles such information. And Congress can create a private right of action against the government to enforce those limits. But it is quite a different matter when, as a means of controlling the Executive, a statute subjects private parties to onerous sanctions for their speech.

The privacy interest that plaintiffs invoke, moreover, is *non*-Constitutional. The Fourth Amendment protects a private zone, defined as "persons, houses, papers, and effects." When one goes outside that private enclave and engages in transactions with third parties, they have their own observations, recollections, and records reflecting those activities. The fact that those interactions have occurred, and evidence obtained from third parties about them, are not private under the Fourth Amendment. *See Smith v. Maryland*, 442 U.S. 735, 745-46 (1979); *Reporter's*

Comm. v. AT&T, 593 F.2d 1030, 1043 (D.C. Cir. 1978); *see also United States v. Forrester*, 2007 WL 2120271, at *6-7 (9th Cir. July 25, 2007) (surveillance of e-mail and website addresses not protected by Fourth Amendment). When privacy interests are extended beyond the Fourth Amendment to prohibit third parties from speaking about their own observations, recollections, and records, their First Amendment rights are set against non-constitutional privacy interests.

A. Defendants' First Amendment Argument Is Narrow

Defendants' First Amendment claim is narrowly based on the specific and unusual facts alleged. Contrary to plaintiffs' hyperbolic claims, Opp. 26-27, defendants' position does not mean that the government is powerless to protect privacy. For example, the government may regulate the disclosure of sensitive information to the public or to private parties for purely commercial purposes. *See Am. Fed'n of Gov't Employees v. HUD*, 118 F.3d 786, 793 (D.C. Cir. 1997) (privacy interest "is significantly less important where the information is collected by the government but not disseminated publicly"); *Trans Union Corp. v. FTC*, 245 F.3d 809, 818, *on reh'g*, 267 F.3d 1138, 1140 (D.C. Cir. 2001) (upholding, under intermediate scrutiny, restriction on sale of credit databases). Such rules present a different First Amendment calculus than is required in this case, in which plaintiffs allege that defendants divulged records to NSA for reasons of the utmost public importance—to help the government protect the nation from attack.

Restrictions on disclosures of client confidences by lawyers and psychiatrists, Opp. 26-27, also present different considerations. Government sanctions on such disclosures must pass muster under First Amendment principles. *See Gentile v. State Bar*, 501 U.S. 1030 (1991) (punishment for violation of ethical rule governing lawyer speech about pending cases subject to First Amendment). But the constitutional calculus in those settings is quite different. Rules regulating disclosures of communications from a patient to his psychiatrist and from a client to her lawyer protect *content* of the most personal and sensitive nature. The confidentiality of such communications is also instrumental to advancing public ends that go beyond the client's individual privacy interests. *See Jaffee v. Redmond*, 518 U.S. 1, 11 (1996) (attorney-client privilege is aimed at "promot[ing] broader public interests in the observance of law and administration of justice," and psychotherapist privilege promotes treatment of mental health

issues, which "is a public good of transcendent importance" (internal quotation marks, alteration, and footnote omitted)). Restricting disclosures by lawyers and psychiatrists is essential to advancing these objectives because clients and patients would not otherwise convey sensitive information. The attorney-client privilege is "the oldest of the privileges for confidential communications known to the common law," *United States v. Zolin*, 491 U.S. 554, 562 (1989), dating "back to the reign of Elizabeth I," 8 J. Wigmore, Evidence § 2290, at 542 (McNaughton rev. 1961). Such "a 'universal and long-established' tradition of prohibiting certain conduct creates 'a strong presumption' that the prohibition is constitutional." *Republican Party of Minn. v. White*, 536 U.S. 765, 785 (2002).

By contrast, call records are far less private than the content of phone calls (OB 36-37)—and less private still than the content of communications with psychiatrists and lawyers. Call records do not contain information communicated by customers, but reflect the telephone company's records of the use of its network. Even a lawyer's records showing that a communication with a client took place—including telephone call records—are not shielded by the attorney-client privilege. *See, e.g.*, *Clarke v. Am. Commerce Nat'l Bank*, 974 F.2d 127, 129 (9th Cir. 1992) (attorney bills not privileged unless they reveal confidences); *Global HTM Promotional Group, Inc. v. Angel Music Group LLC*, 2007 WL 221423 (S.D. Fla. Jan. 26, 2007) (phone records of calls between lawyer and client not privileged). Barring disclosure of call records, moreover, is not aimed at, let alone essential to, promoting public ends in the same way as are the attorney-client and psychotherapist-patient privileges.

In addition, ECPA's prohibition is neither long-standing nor voluntarily assumed. For most of their history, telephone companies were not restricted from communicating records to the government. *See Reporter's Committee*, 593 F.2d at 1036. ECPA imposed a new prohibition, whose validity as applied must be evaluated under established First Amendment standards. Telephone companies cannot be said to have "voluntarily" assumed ECPA's restrictions just by continuing to do business after it was enacted. Opp. 37. Telephone companies were not only legally prohibited from ceasing to operate (*see, e.g.*, Cal. Pub. Util. Code § 451), but also were compelled to continue operating in order to recover their sunk costs.

Plaintiffs' suggestion that one "voluntarily" submits to a law by acting after the law is enacted—that the law is valid because the law exists—is flatly inconsistent with the well-established rule that one cannot constructively consent to the surrender of constitutional rights. In *College Savings Bank v. Florida Prepaid Postsecondary Education Expense Board*, 527 U.S. 666 (1999), the Court applied this principle to hold that states did not waive their sovereign immunity by merely engaging in conduct regulated by federal law. Even the government acknowledged that such a waiver would not be voluntary if the law applied to activities that the state "cannot realistically choose to abandon," *id*. at 679—a rule that would apply to defendants, which could not realistically cease operating. The Court went further, however, holding that states cannot "constructively waive" sovereign immunity—just as individuals cannot "constructively waive" their constitutional rights—even where they engage in the regulated activity voluntarily. *Id*. at 681-82. The very idea of "constructive" waiver of a constitutional right, the Court explained, is "unheard of." *Id*. at 681. Congress cannot circumvent the Constitution's limits on its ability to take away rights by casting its action in the form of a condition, for "*all* federal prescriptions are, insofar as their prospective application is concerned, in a sense conditional, and—to the extent that the objects of the prescriptions consciously engage in the activity or hold the status that produces liability—can be redescribed as invitations to 'waiver.'" *Id*. at 683 (citation omitted). The notion of voluntary acceptance of a restriction, moreover, presupposes that the government is providing some benefit in exchange. *Id*. at 686.[1] But in ECPA, as in the statute considered in *College Savings*, "what Congress threatens if the [defendant] refuses to agree to its condition is not the denial of a gift or gratuity, but a sanction: exclusion of the [defendant] from otherwise permissible activity." *Id*. at 687.[2]

[1] Thus, the government may condition the grant of the privilege of public employment on speech restrictions, within constitutional limits. *See Connick v. Myers*, 461 U.S. 138, 147 (1983). *United States v. Aguilar*, 515 U.S. 593 (1995), cited in Opp. 37, falls within this line of authority. *Aguilar* observed that "[g]overnment officials in sensitive confidential positions may have special duties of nondisclosure." *Id*. at 606. Thus, a requirement that a judge maintain the confidentiality of information learned in the course of his duties was voluntarily assumed when the judge accepted his Article III commission. *Id*. The Court was careful to distinguish that situation from "efforts to impose restrictions on unwilling members of the public," *id*., as are imposed by ECPA.

[2] Plaintiffs cite Richards, *Reconciling Data Privacy and the First Amendment*, 52 UCLA L. Rev.

As indicated in *College Savings*, a constructive waiver rule would eviscerate the First Amendment. It would justify a law prohibiting a trade association from lobbying legislators with information obtained from a source funded by its members, or a law prohibiting the press from publishing information obtained from a government employee. No case has suggested that such blatantly illegal prohibitions are exempt from constitutional scrutiny if enacted before the expression occurred, and myriad cases are to the contrary. *See, e.g., U.S. West, Inc. v. FCC*, 182 F.3d 1224 (10th Cir. 1999) (restriction on telephone companies' use of call records subject to First Amendment scrutiny); *Fla. Star v. B.J.F.*, 491 U.S. 524 (1989) (law prohibiting publication of victim's name obtained from public records subject to First Amendment scrutiny).

Plaintiffs' alarmist rhetoric about the threat to other privacy laws, Opp. at 25-27, is baseless. The cited statutes permit disclosures for national security or law enforcement purposes and/or are otherwise distinguishable, as discussed in the margin.[3]

1149, 1201-08 (2005), which argues that the First Amendment imposes no limitation on most laws restricting disclosures of data. *See* Opp. 27 n.27. Even plaintiffs cannot bring themselves to endorse this author's argument, and for good reason. To begin with, the article addresses sales of data for commercial purposes, not the communication of data on matters of public importance, as alleged in this case. The author's interpretation of the First Amendment is also inconsistent with settled law. The author argues that legislatures are as free to prohibit businesses from communicating information about transactions with their customers as legislatures are to impose rules rendering unenforceable contracts with an incompetent counter-party. 52 UCLA L. Rev. at 1203-04. This does not follow. In the former situation, the law implicates the companies' First Amendment rights, a position that even plaintiffs do not contest. In the latter, it does not.

[3] Regulations implementing the Health Insurance Portability and Accountability Act ("HIPAA") permit health care providers to disclose "protected health information to authorized federal officials for the conduct of lawful intelligence, counter-intelligence, and other national security activities authorized by the National Security Act . . . and implementing authority. . . ." 45 C.F.R. § 164.512(k)(2). Those regulations also allow providers to disclose certain basic information about patients, such as their name, address, and date and time of treatment, in response to a law enforcement official's request for the purpose of identifying or locating a suspect. *Id.* § 164.512(f)(2). In any event, the privacy interests at stake with the health information covered by HIPAA—personal medical information, including the substance of a patient's communications with her doctor—are far different than those at issue with regard to telephone records. The Fair Credit Reporting Act ("FCRA") does not prohibit financial institutions from providing consumer identifying information to the government, even without a request. 15 U.S.C. § 1681f. In addition, FCRA does not restrict the provision of reports of transactions or experiences between the consumer and the person making the report, *id.* § 1681a(d)(2)(A)(i), which is the analogue to call records reflecting transactions between a customer and a telephone company. The Family Educational Rights and Privacy Act ("FERPA") only conditions the receipt of federal funds on certain disclosure limits; it is not a direct prohibition on providers like ECPA. *See Rust v. Sullivan*, 500 U.S. 173, 179-80 (1991) (upholding restrictions on counseling concerning abortion based on government's right to condition federal funds). In any case, FERPA does not prohibit educational institutions from disclosing student records to the Attorney General's representatives

B. Defendants Cannot Be Held Liable for Their Alleged Speech

A prohibition on truthful speech lawfully acquired is subject to exacting First Amendment scrutiny regardless of the content of the speech. But when a prohibition is applied to speech that involves a matter of public concern and/or is political, strict scrutiny is clearly the appropriate standard. Plaintiffs debate the applicable standard of review, Opp. 27-35, but ECPA cannot constitutionally be applied to the facts alleged under *any* First Amendment standard, and at least would raise a serious constitutional question that can, and must, be avoided by construing ECPA as not applying to the facts alleged.

Plaintiffs do not dispute that prolonged litigation can chill First Amendment rights and that disposition of a complaint based on alleged conduct protected by the First Amendment on a motion to dismiss is particularly important. OB 26-27. Requiring a speaker to undergo discovery about its subjective motives "constitutes a severe burden on political speech" and would "unquestionably chill a substantial amount of political speech." *FEC v. Wis. Right to Life, Inc.*, 127 S. Ct. 2652, 2666 & n.5 (2007) ("*WRTL*") (opinion of Roberts, C.J., joined by Alito, J.).

1. *Applying ECPA to the Facts Alleged Would Fail Strict Scrutiny*

A content-neutral prohibition, when applied to speech that is of public concern or political, is subject to strict scrutiny. Thus, a restriction on attorney solicitation is usually subject to intermediate scrutiny, but is subject to strict scrutiny when applied to the ACLU's solicitation of clients in civil rights cases, an activity that involves core political speech. *In re Primus*, 436 U.S. 412, 432 (1978). *Primus* reached this conclusion without discussing whether the restriction was content-based. *See also Board of Trustees v. Fox*, 492 U.S. 469 (1989) (restriction subject to intermediate scrutiny when applied to commercial speech, but higher level of scrutiny as applied

---

for law enforcement purposes. 20 U.S.C. § 1232g(b)(1)(C)(ii). Finally, the Uniform Trade Secrets Act ("UTSA") prohibits disclosure of secret information that belongs to another person. Uniform Trade Secrets Act § 1(2)(ii). By contrast, call records are created by, and are the property of, telephone companies. In any case, trade secret laws like the UTSA are subject to First Amendment scrutiny. *See, e.g.*, *Ford Motor Co. v. Lane*, 67 F. Supp. 2d 745, 749-50 (E.D. Mich. 1999). *DVD Copy Control Ass'n v. Bunner*, 31 Cal. 4th 864 (2003), on which plaintiffs rely, Opp. 35, applied intermediate scrutiny to an injunction against disclosure of a trade secret. The court distinguished *Bartnicki* and upheld the injunction principally on the ground that the disclosure of the trade secret did *not* involve a matter of public importance. 31 Cal. 4th at 883.

to non-commercial speech; no discussion of whether restriction was content-based); OB 32-33.

a. *The Speech Alleged Would Be of Public Concern and Political*

The speech alleged would have been of public concern. OB 33. Cases holding that the sale of data for commercial purposes does not involve speech of public concern are inapposite. Opp. 35. The Complaint does not claim that defendants' alleged speech was "solely in the individual interests of the speaker and its specific *business* audience," *Dun & Bradstreet, Inc. v. Greenmoss Builders, Inc*., 472 U.S. 749, 762 (1985) (plurality) (emphasis added); that it was "*solely* motivated by the desire for profit," *id*. (emphasis added); or that it was false, *id*. Instead, the Complaint alleges that defendants divulged records for the "purpose of assisting the government" in its efforts to prevent terrorist attacks (Compl. ¶ 259)—a matter of grave societal importance. OB 33. Defendants' status as commercial entities, Opp. 35, is irrelevant. Speech is protected because of its "inherent worth," regardless of whether it is uttered by an individual or a for-profit corporation. *First Nat'l Bank of Boston v. Bellotti*, 435 U.S. 765, 777 (1978).

The speech alleged would address a matter of broad public importance, as is definitively established by the common law privilege for providing information relating to public safety: communications privileged at common law are by definition of public concern. OB 33.

The speech alleged in the Complaint also would be "political," i.e., designed to influence government action. *Id.* Plaintiffs do not rebut this point but claim that the standard of review for time, place, and manner restrictions is based on the restriction at issue, not the speech to which it applies. Opp. 34 n.35. But an outright *ban* on speech is not a time, place, and manner restriction. As noted, under *Primus* and *Fox*, a ban on speech is evaluated differently when applied to political speech than it is when applied to commercial speech.

b. *The Volume of Data Allegedly Communicated Does Not Change Its Protected Character*

Plaintiffs imply that many of the call records allegedly communicated were not of public concern because they pertained to customers with no link to terrorists. Opp. 34-35, 41-42. Based on the allegations of the Complaint, however, the volume of data allegedly communicated does not change its character as of public concern and political.

In the context of ordinary law enforcement activities, in those cases in which the government has already identified a suspect, the information sought by the government and provided by private parties can frequently be limited to a specific individual. In other criminal investigations, however, when the government does not know the identity of the culprit, it usually needs access to broader categories of information in order to narrow the range of possible suspects. In such cases, to determine who has committed certain acts, the investigator typically looks for correlations between different sets of data. For example, in the case of the Washington sniper, comparing license plate numbers of cars seen on security cameras near one shooting site with those seen at a second site could establish a "match" and thus potentially identify a suspect. In the workaday criminal law enforcement context, many examples of this technique arise every day, as the police run fingerprints found at the scene against a fingerprint database, or examine hotel registries, rental car records, databases of gun purchases, etc. In conducting such cross-analysis, *all* data needed to enable that comparison are relevant; the data not ultimately matched permit the match to be made through the process of inclusion and exclusion. Thus, in the law enforcement context, data that may yield directly relevant information are themselves "relevant" unless "there is *no reasonable possibility* that the category of materials the Government seeks *will produce* information relevant to the general subject of the grand jury's investigation." *United States v. R. Enters.*, 498 U.S. 292, 301 (1991) (emphasis added).

From the speaker's perspective, speech is of public concern if there is a reasonable basis for believing that the information communicated would be useful in protecting the public. Whatever may be said about the predicate for the government to search for information, a speaker need not have "individualized suspicion" that particular information is linked to a specific suspect. Opp. 36. For example, if a farm supply company decides to give the government records of purchasers of ammonium nitrite fertilizer that can be used to create explosives, so that the government can cross-check those records against a terrorist watch list, the company's speech would be of public concern, even though the vast majority of purchasers would be innocent.

Accepting the allegations of the Complaint as true, *all* of the call records allegedly communicated to the government would have been relevant—and hence all of public concern and

political—because they allegedly enabled the government to identify terrorists through the process of inclusion and exclusion. OB 3 (summarizing allegations of Complaint). Moreover, the facts alleged establish, as a matter of law, that all of the alleged speech would be fully protected because plaintiffs allege that the government requested it in the context of a declared emergency. Plaintiffs do not dispute that, under the circumstances they allege, it would have been objectively reasonable for private parties to rely on the government's judgment as to what information would be relevant to the task at hand. OB 42.

Finally, plaintiffs' argument runs directly into state secrets. If the alleged program existed, and if NSA required access to all of the records allegedly obtained in order to prevent terrorist attacks, then plaintiffs' assertion that the alleged communication of records was not of public concern would fail. The Complaint alleges all the facts requisite to finding that the records allegedly communicated were of public importance, but if additional facts about NSA's alleged operations were required, the state-secrets privilege renders them unavailable.

c. *ECPA's Prohibition Is Content-Based*

The speech alleged is so clearly of public concern that there is no need to dwell on why ECPA is content-based. The test for whether a law is content-based, however, is not a free-form inquiry into legislative purpose. Opp. 28-29. More recent cases have made clear that the test is based on whether the statute describes speech by content and whether it contains content-based exceptions that involve the same potential harms. OB 34; *see also Bartnicki v. Vopper*, 532 U.S. 514, 523 n.9 (2001) ("while a content-based purpose may be sufficient in certain circumstances to show that a regulation is content based, it is not necessary to such a showing in all cases").

d. *Applying ECPA to the Facts Alleged Is Not the Least Restrictive Alternative to Advancing a Compelling Interest*

A prohibition on truthful speech about information lawfully acquired on a matter of public concern fails strict scrutiny. The Supreme Court has repeatedly held that privacy interests are not sufficient to justify such a prohibition, even when privacy interests are much stronger than those alleged by the Complaint. OB 35-36. Moreover, the interest in preventing the government's misuse of information can be served by the less restrictive means of limiting the government

rather than the speaker. OB 35-39. Plaintiffs do not suggest that ECPA's prohibition, as applied to the facts alleged in this case, would survive strict scrutiny.

2. *Applying ECPA to the Facts Alleged Would Fail Intermediate Scrutiny*

ECPA, as applied to the facts pled, also would fail intermediate scrutiny—one of the standards *plaintiffs* propose. Opp. 30. Under this standard, plaintiffs must show that ECPA directly advances a substantial governmental interest. OB 40; Opp. 38. This requires plaintiffs to identify an interest outside ECPA that the statute is designed to advance. It is circular to suggest that ECPA *creates* a privacy interest that the government has a substantial interest in protecting.

The specific privacy interest that plaintiffs claim ECPA is protecting *in this case* is not substantial. Plaintiffs do not claim that the government publicized or misused information about them, or even that an excessive number of government employees saw such information. As plaintiffs tacitly admit, if that were the harm claimed, the more narrowly tailored solution would be to restrict the actions of government employees. OB 39; Opp. 39. Nor do plaintiffs claim that they suffered a dignitary harm of a government employee examining their call records. Plaintiffs do not claim that their records were linked to terrorists and extracted for human examination. Instead, plaintiffs claim that they are entitled to recover if records about their calls were placed into a database that was queried by a computer, even though records about their calls, under the facts alleged, were not examined by any human being. That is not a substantial privacy interest. *See Warshak v. United States*, 2007 WL 1730094, at *14 (6th Cir. June 18, 2007) (expectation of privacy in the content of e-mails is not diminished by providers' use of computers to screen emails because "[t]he fact that a computer scans millions of e-mails for signs of pornography or a virus does not invade an individual's content-based privacy interest in the e-mails ...").

While plaintiffs refer to the importance of privacy in general, Opp. 30, they do not cite any authority to support their claim that the specific privacy harm they allege is substantial. Plaintiffs cannot meet their burden of showing a substantial interest "merely [by] asserting a broad interest in privacy. [They] must specify the particular notion of privacy and interest served." *U.S. West*, 182 F.3d at 1235. In applying intermediate scrutiny to restrictions on the use

of call records for commercial purposes, *U.S. West* stated: "In the context of a speech restriction imposed to protect privacy by keeping certain information confidential, the government must show that the dissemination of the information desired to be kept private would inflict specific and significant harm on individuals, such as undue embarrassment or ridicule, intimidation or harassment, or misappropriation of sensitive personal information for the purposes of assuming another's identity." *Id*. Absent specific evidence that call records would be disclosed to people in a manner that would cause customers to suffer such "specific and significant" harms, the restriction on disclosure was invalid. *Id*. Although *U.S. West* was featured prominently in our opening brief, OB 38 & 40, plaintiffs offer no response.

Nor do plaintiffs show that applying ECPA's prohibition directly advances a substantial interest in promoting *private* speech. Opp. 31, 45. First, plaintiffs do not demonstrate any nexus between divulgence of call records and private speech. While plaintiffs cite authorities suggesting that interception of call *content* (i.e., surveillance) can chill private speech, *id*. at 31 (citing *Bartnicki*), none of those authorities extends this conclusion to call *records*. Plaintiffs' speculation that divulgence of records would chill speech is inadequate. *See Edenfield v. Fane*, 507 U.S. 761, 770 (1993) ("burden is not satisfied by mere speculation or conjecture"). Plaintiffs' speculation lacks credibility in any case. Under ECPA, various government agencies can compel production of call records by issuing an administrative subpoena or by other means. 18 U.S.C. § 2703(c). There is no reason to believe that a customer would be more chilled if he knew that his records were placed into a database and extracted only if linked to a terrorist, as plaintiffs claim. Second, an interest in promoting private speech cannot justify suppressing speech on a matter of public concern. That was the precise holding of *Bartnicki*, 532 U.S. at 534. Even if plaintiffs could show that divulgence of records chills private speech, that rationale would not justify applying ECPA to the facts alleged. Third, plaintiffs' suggestion that the interest in promoting private speech involves a competing *constitutional* right, Opp. 45, is incorrect. Not only have plaintiffs failed to show that the alleged divulgence of records chills private speech, but such a chill would not amount to a First Amendment violation. Even the government does not infringe First Amendment rights by engaging in surreptitious intelligence-gathering as part of a

bona fide investigation, particularly where the Fourth Amendment is not at stake. *See United States v. Mayer*, 2007 WL 1760668, at *8-9 (9th Cir. June 6, 2007) (First Amendment does not restrict investigation conducted for a legitimate law enforcement purpose; "the First Amendment does not expand the criminal procedure protections provided by the Fourth Amendment").

3. *Applying ECPA to the Facts Alleged Would Violate the First Amendment under* Bartnicki

ECPA's application to the facts pled also would violate the First Amendment under plaintiffs' preferred approach—the *Bartnicki* standard. Opp. 35-38. As compared to the discussion of a labor negotiation in *Bartnicki*, the speech alleged in the Complaint, which allegedly was aimed at protecting the nation from terrorist attack, would have been of even greater public importance. On the other side of the scale, the privacy interest in call records is far weaker than in call content at issue in *Bartnicki*. And the privacy interest alleged by plaintiffs—preventing records from being scanned by a computer—is particularly weak.

The Fourth Amendment norm against dragnet searches not based on individualized suspicion, Opp. 36, is inapplicable. That norm is directed at government searches, not speech by private parties. In addition, unlike the interception of calls, the collection of call records does not implicate the Fourth Amendment. Moreover, plaintiffs allege that computers were used to sift a large volume of data. If true, that would be a minimization technique that is the very opposite of a dragnet. It would allow the isolation and extraction of the information needed without human examination of the remainder: The needle could be plucked from the haystack without anyone looking through the hay. "Rather than invading privacy, computer sifting prevents most private data from being read by an intelligence officer or other human being by filtering them out." Posner, Not a Suicide Pact: The Constitution in a Time of National Emergency 97 (2006).

ECPA refutes plaintiffs' argument that privacy outweighs speech under the facts pled. ECPA itself strikes the relevant balance: privacy interests must give way when records are relevant to a broad array of investigations, from those involving telemarketing fraud (§ 2703(c)(1)(D)) to those involving international terrorism (§ 2709). OB 38. Privacy interests cannot outweigh the right of a private party to engage in constitutionally protected speech by

communicating information to the government relevant to such an investigation, as the Complaint alleges. Plaintiffs' contention that there is no third party to be regulated, Opp. 37-38, is incorrect as applied to the facts pled. If ECPA prohibits disclosure in these alleged circumstances, it is only because the government allegedly failed to issue a subpoena or other legal process. That may be a reason to punish the government, but it is not a reason to muzzle the alleged speaker.

Finally, Verizon's privacy policy does not constitute a voluntary acceptance of ECPA's restrictions. The quoted policy, Opp. 37, simply refers to the existence of 47 U.S.C. § 222 (not ECPA), and, as noted, one does not "voluntarily accept" the obligations of a law by acknowledging its existence. *See also infra* at 36 (discussing privacy policy).

C. The Alleged Communication of Records Is Protected by the Petition Clause

Plaintiffs admit that the alleged communication of records was speech but deny that it was petitioning activity. It is difficult to imagine speech directed to the government that would not be a petition, but the speech alleged clearly would be a petition. The Complaint alleges that defendants communicated records to NSA for the purpose of helping the government protect the country from further terrorist attacks. Compl. ¶ 259. In these alleged circumstances, defendants' alleged petition would have had two elements: (1) "We believe that the records we are communicating may be useful in finding terrorists," and (2) "Please use them for this purpose."

Plaintiffs concede that the Petition Clause *would* protect defendants' right to tell the government that their call records could help identify terrorists and to ask the government to use those records for that purpose, but they claim that defendants can be prohibited from presenting the records themselves until the government compels their production. Opp. 41. This contention fails for three reasons. First, the Petition Clause protects the right to communicate facts to the government. OB 29. Specifically, communicating facts to law enforcement is protected by the Petition Clause. *Forro Precision, Inc. v. IBM Corp.*, 673 F.2d 1045, 1060 (9th Cir. 1982); *see also* OB 29-30 (collecting cases). Plaintiffs fail to point to any language in those cases, or to cite any other authority, that would support their assertion that this protection applies only if the information supplied shows that a particular customer committed a wrong. *See* Opp. 41-42. Nor could they: the Petition Clause protects the right to communicate information to the government

that could be useful in protecting public safety, whether the source of the threat is known or yet to be isolated. OB 29. The right to provide information that helps the government identify persons threatening to inflict harm on the public has always been recognized at common law, was affirmed as a fundamental constitutional right in *In re Quarles*, 158 U.S. 532 (1895), and is enshrined in the Petition Clause as a personal right, integral to self-governance. OB 30-31.

Second, the petitioner has the prerogative to decide what to include in a petition. The Petition Clause protects a constituent's right not only to ask her Member of Congress to cap greenhouse gas emissions, but also to present scientific data showing that such emissions harm the environment. A petitioner's ability to submit a different—and potentially less effective—petition does not give the government the power to prohibit the presentation of the information that the petitioner chooses to submit. *See WRTL*, 127 S. Ct. at 2671 n.9 (Roberts, C.J., joined by Alito, J.) (the argument "that corporations can still speak by changing what they say to avoid mentioning candidates . . . is akin to telling Cohen that he cannot wear his jacket because he is free to wear one that says 'I disagree with the draft,' or telling 44 Liquormart that it can advertise so long as it avoids mentioning prices. Such notions run afoul of 'the fundamental rule of protection under the First Amendment, that a speaker has the autonomy to choose the content of his own message'" (citations omitted)); *In re IBP Confidential Bus. Documents Litig.*, 797 F.2d 632, 641 (8th Cir. 1986) (en banc) ("[the petitioner], rather than [the government], has the right to determine how and in what manner [the] right [to petition] will be exercised").

Third, conditioning the right to present facts to the government on the government's discretion to take steps to compel its production would be an invalid prior restraint. OB 28-29.

The Petition Clause protects the right to present facts not only when they are actually useful in protecting public safety, but also when there is an objectively reasonable basis to believe they would be. OB 31, 41. An objectively reasonable person would have been entitled to rely on the government's purported representation that the records allegedly requested would be useful in preventing terrorist attacks. OB 41-42. Plaintiffs do not respond to this critical point.

Even if the alleged communications of call records were not petitions, they would be protected as activity "incidental to" petition. OB 31; *Sosa v. DIRECTV, Inc.*, 437 F.3d 923, 934

(9th Cir. 2006). A wide range of activity ancillary to a petition is protected, such as pre-suit demand letters among private parties, *Sosa*, 437 F.3d at 933; out-of-court discovery conduct, *Freeman v. Lasky, Haas & Cohler*, 410 F.3d 1180, 1185 (9th Cir. 2005); and a non-party's financing of litigation, *Liberty Lake Investments, Inc. v. Magnuson*, 12 F.3d 155 (9th Cir. 1993). If the Petition Clause protects interactions between private parties, it clearly protects the communication of information to the government. And the "breathing space" around petitions is even wider when it comes to assisting law enforcement. *See* OB 31-32. Plaintiffs' contrary suggestion, *see* Opp. 44 n.39, misreads the law. *See Kottle v. Northwest Kidney Ctrs.*, 146 F.3d 1056, 1062 (9th Cir. 1998) ("the sham *exception* [to *Noerr-Pennington*'s protection] is *narrower* in communications with the police than it is in the legislative realm" (emphases added)). Under the breathing space principle, defendants' alleged activity was protected as activity incidental to petitions even if the information allegedly supplied was broader than necessary. OB 32.

Because the Complaint seeks to impose liability for alleged conduct that would be protected by the Petition Clause, the records claims must be dismissed. *See, e.g.*, *Kottle*, 146 F.3d at 1058-59. At a minimum, the Court must, if possible, interpret ECPA as not prohibiting the conduct alleged.

IV. ECPA CAN AND MUST BE CONSTRUED NOT TO APPLY

The constitutional issues discussed above trigger *Ashwander*'s canon of avoidance. A "grave doubt" about the constitutionality of applying ECPA to the facts alleged is not required. Opp. 44-45. Rather, in the Ninth Circuit, *Ashwander* applies whenever the application of a statute "'presents a *significant risk* that the First Amendment will be infringed,'" even if the violation is not "probabl[e]." *Overstreet v. United Bhd. of Carpenters & Joiners of Am.*, 409 F.3d 1199, 1209 (9th Cir. 2005) (emphasis added, citation omitted). Likewise, the clear statement rule requires construing a statute not to apply unless Congress has made its intent to regulate the President's exercise of Article II power unequivocally clear. Accordingly, the Court must adopt a construction of ECPA that avoids these constitutional problems "unless the statute clearly provides otherwise." *Sosa*, 437 F.3d at 931 (applying *Noerr-Pennington* doctrine). If the statute

does not "directly" and "unambiguously" impose liability for the conduct alleged, *id*. at 940, the statute must be construed as not applying. Plaintiffs have not met their heavy burden of showing that it is impossible to interpret ECPA as not imposing liability for the conduct alleged.

As shown above, the most straightforward way of complying with these principles is to conclude that ECPA does not apply to the President's collection of records for national security intelligence purposes, as alleged in the Complaint. *See supra* at 2-5. Alternatively, the Court can construe specific provisions of ECPA as barring the claims. Plaintiffs cannot avoid this conclusion simply by relying on conclusory legal allegations. Because the *facts* alleged establish that ECPA's prohibition does not apply, the Complaint's contrary legal allegations, *see* Opp. 22, must be disregarded. *See Rutman Wine Co. v. E. & J. Gallo Winery*, 829 F.2d 729, 736 (9th Cir. 1987) ("merely alleging a bare legal conclusion" insufficient); *Cholla Ready Mix, Inc. v. Civish*, 382 F.3d 969, 973 (9th Cir. 2004) ("court is not required to accept legal conclusions cast in the form of factual allegations if those conclusions cannot reasonably be drawn from the facts alleged" (internal quotation marks omitted)).

A. ECPA's Prohibition on "Divulgence" Does Not Apply to the Facts Pled

"Divulge," as used in 18 U.S.C. § 2702(a)(3), is a term of art that means to make previously secret information known to another. OB 23-24. Thus, in the two-step process that plaintiffs allege, records would not be "divulged" within the meaning of § 2702 when placed into a database that can be queried; only those records that a computer identifies as linked to a terrorist and therefore selects for human examination would be subject to the statute's prohibition. *Id*.

Plaintiffs do not dispute that "divulge" means to make secret information known to another person. OB 22. Instead, plaintiffs resort to a sleight-of-hand. Rather than address the meaning of divulge directly, they point to other portions of ECPA that use the term "disclose" to refer to the prohibition on divulgence and claim that "disclose" has a broader meaning. But as plaintiffs admit, "disclose" has *two* meanings. Its primary meaning is the same as "divulge," i.e., to make known. It also has a secondary meaning of exposing to view, which it does *not* share with divulge. Opp. 22 ("'disclose,' while *sharing* the definition 'to make known' with 'divulge,' *also* is defined as 'to expose to view …'" (emphasis added)). Thus, ECPA's references to

"disclose" can and must be read in harmony with the plain meaning of "divulge." Plaintiffs do not cite any source that defines "divulge" as meaning merely uncovering or giving access. In fact, the dictionary they cite defines "divulge" exclusively as "[t]o make known (something private or secret)." American Heritage Dictionary (4th ed. 2000). Nor is the meaning of divulge altered because the word "provide" appears in a single sentence in a congressional committee report. Opp. 23 (citing H.R. Rep. No. 99-647, at 64 (1986)). This passing reference cannot change the plain meaning of divulge, nor is there any indication that Congress meant to do so.

The statute's structure confirms this conclusion. ECPA uses different language to prohibit "access" to facilities that store information. OB 25 (discussing § 2701(a)). Congress meant to refer to a different and narrower action when it separately prohibited divulgence. Plaintiffs' view that divulgence occurs whenever access is provided, Opp. 22, is refuted by this structure, and by the grammatical structure of § 2702(a)(3), which refers to divulging "a" record about "a" subscriber, not providing access to a system of records. OB 25. Plaintiffs do not address these points, or the Ninth Circuit's comment that "[a]ccess does not necessarily mean disclosure." *Planned Parenthood of S. Ariz. v. Lawall*, 307 F.3d 783, 789 n.5 (9th Cir. 2002).

Extrinsic guides to construction confirm the plain meaning of divulge. While plaintiffs protest that referring to libel law to help construe a privacy statute is "absurd," Opp. 3, that is precisely what the Ninth Circuit expressly held is appropriate. *Oja v. U.S. Army Corps of Eng'rs*, 440 F.3d 1122, 1129 (9th Cir. 2006). A libel is not "published"—the analogue of "divulged"—unless it is apprehended by another; placing information into a computer or other place where it can be accessed is not sufficient. OB 24. Plaintiffs do not suggest that libel law provides otherwise. Instead, plaintiffs refer to "intrusion upon seclusion," Opp. 23-24, but that tort protects against a different kind of action: encroaching into a private place in a way that would be highly offensive to a reasonable person (e.g., a tabloid photographer forcing his way into a celebrity's hotel room). *See* Restatement (Second) of Torts § 652B (1977); *id.*, cmt. b. Plaintiffs have not alleged that defendants impermissibly viewed their phone records, nor could they given that phone records are created by, and are the property of, defendants. *See id.*, cmt. c (intrusion on seclusion tort applies only where defendant "has intruded into a private place"); *In re Trans*

Union Corp., Privacy Litig., 326 F. Supp. 2d 893, 902 (N.D. Ill. 2004) (credit reporting company accessing its own files of information about consumers not an intrusion).[4] Intrusion upon seclusion does not govern the separate action of divulging information to a third party.

Plaintiffs argue that ECPA is directed solely at regulating providers, regardless of the actions of government agents. Opp. 23. They also say that the Court decided the meaning of "divulge" in *Hepting v. AT&T*, 439 F. Supp. 2d 974, 999 (N.D. Cal. 2006), even though the Court was not then considering this question. Section 2702(a)(3) does apply solely to providers, but it prohibits only those acts that result in making information known to government agents. The provider's offense is not complete until the information is apprehended. In this way, the term "divulge" delimits and defines the scope of the dignitary harm protected by ECPA. ECPA's focus on the actions of the provider is not at odds with its requirement that the plaintiff show that information was made known to another, any more than libel law's restrictions on speakers are inconsistent with the requirement that a plaintiff show that the libel was apprehended.

Plaintiffs next shift ground and claim that ECPA is not concerned solely with the provider but is directed at restraining the government. Opp. 24. Plaintiffs invoke the Fourth Amendment value against general warrants and claim that ECPA should be read to constrain government agents' "unchecked discretion" to review records because this creates the risk of abuse. *Id*. This argument supports our First Amendment claim: if ECPA's purpose is to prevent government abuse, the only solution compatible with the First Amendment is to control the government rather than the alleged speaker. As it relates to the meaning of divulgence, plaintiffs' argument fails. First, their hypothesis that § 2702(a)(3) is designed to address the risks flowing from government access is refuted by the statute's use of the term "divulge." As noted, divulge is not equivalent to access. Second, the Fourth Amendment does not apply to telephone records or to actions of private parties. Third, plaintiffs have not alleged that NSA analysts have unchecked discretion to examine records. The Complaint alleges that records were provided for the purpose of enabling

[4] Plaintiffs purport to quote the "holding" of *Shulman v. Group W Productions, Inc.*, 18 Cal. 4th 200, 232 (1998), Opp. 23, but the words their parenthetical puts in quotation marks do not appear in the opinion.

the identification of terrorists, and that the records were subject to a winnowing process directed at that end. The Complaint alleges that the records were subjected to a system of *selective* access, in which records are queried by computers and humans examine them only if they are linked to terrorists. *See* OB 22-23 (summarizing allegations of Complaint). If the alleged records program operated as plaintiffs claim, only the records extracted would be made known to government agents. Indeed, the Complaint does not allege that the records identified customers. OB 25-26. Plaintiffs' claim thus boils down to the extreme and unsupportable proposition that divulgence occurred simply because records allegedly were included in a database that allegedly was queried by a computer—even though, according to the Complaint's allegations, plaintiffs' records were not and *could not be* examined by a human because they were not linked to terrorists. Fourth, even if plaintiffs had alleged that NSA could obtain access to records on other terms, this would require plaintiffs to delve into NSA's alleged operations, including the terms under which NSA analysts allegedly could gain access to the alleged database and the reasonableness of the search criteria. If a records program existed, these would be highly secret matters, litigation of which would be barred by the state-secrets doctrine.

ECPA's prohibition on divulgence is properly construed as not extending to records not examined by humans. At a minimum, ECPA does not clearly foreclose that interpretation. Plaintiffs' own arguments—that "disclose" has two meanings and that the legislative history should be consulted—confirm that the prohibition on divulgence does not *unambiguously* cover access without examination. Accordingly, ECPA can and must be construed not to apply in order to avoid the serious constitutional issues that would otherwise arise.

B. ECPA's Exceptions Apply to the Facts Pled

ECPA's emergency and rights and property exceptions also apply to the conduct alleged. Plaintiffs' suggestion that defendants have the burden of proving that these exceptions apply, Opp. 5, is incorrect but irrelevant at this stage. The Complaint alleges facts establishing that the emergency and rights and property exceptions apply. At a minimum, under the doctrine of constitutional avoidance, those exceptions must be so construed.

1. *The Emergency Exception Applies Under the Facts Alleged*

The allegations of the Complaint establish that there was an emergency that was both "immediate" under the 2001 version of ECPA and required a response "without delay" under the 2006 version. *See* Opp. 8-9 & n.10. Plaintiffs allege that defendants disclosed records to NSA after the President had declared that the threat of another terrorist attack was an "emergency" and that there was a "continuing and *immediate* threat of further attacks." OB 21 (emphasis added). The President has renewed that declaration annually. *Id.* Congress similarly found that terrorism poses "an unusual and extraordinary threat to national security." *Id.* Plaintiffs have made no attempt to contest that these judgments by the political branches establish *as a matter of law* that the prospect of a terrorist attack constituted an emergency. Beyond these findings, a terrorist attack by definition is an emergency, i.e., a "sudden unexpected happening." Black's Law Dictionary 522 (6th ed. 1990). Because the timing of a terrorist attack is inherently uncertain, any attack would be sudden and unexpected and hence an emergency. And because an attack could be launched at any time, information relating to its prevention must be provided "without delay." This is the most reasonable construction of ECPA, and certainly is not unambiguously foreclosed.

The Complaint's allegations also establish that the information allegedly disclosed "relat[ed] to" the emergency. That phrase, as used in the 2006 version of § 2702(c)(4), does not limit disclosures to records of calls made by the person who is threatening harm, as plaintiffs erroneously suggest. Opp. 9 n.10. Instead, it authorizes disclosure of records that "ha[ve] a connection with, or reference to" the emergency. *Morales v. Transworld Airlines*, 504 U.S. 374, 383 (1992) (so characterizing "the ordinary meaning" of "relating to"). The allegations of the Complaint themselves establish the requisite relation: Plaintiffs claim that records were provided at NSA's request for the purpose of enabling NSA to prevent terrorist attacks.

These allegations, and the findings of the political branches, also establish that defendants would have had a reasonable or good faith belief that an emergency justified the disclosures alleged. "Reasonable," the term used in the 2001 version of ECPA, Pub. L. No. 107-56 § 212, 115 Stat. 272 (2001), inherently connotes an objective standard. "Good faith," which appears in

the 2006 version of ECPA, also can be construed as an objective standard. *See, e.g.*, *Coppedge v. United States*, 369 U.S. 438, 445 (1962) ("good faith" in context of statute governing in forma pauperis appeals "must be judged by an objective standard"). The constitutional issues raised by the Complaint's allegations, moreover, require the exception to be construed to authorize disclosures based on an objective standard. The President's constitutional power to collect intelligence cannot be made to depend on a provider's motives. OB 22. Likewise, under the First Amendment, liability cannot be imposed if there is an objectively reasonable basis for believing that the speech or petition was lawful. A speaker cannot be required to undergo the costly and uncertain process of demonstrating its subjective state of mind if there was an objectively reasonable basis for believing its speech was lawful. *See Prof'l Real Estate Investors v. Columbia Pictures Indus., Inc.*, 508 U.S. 49, 57 (1993) (an "objectively reasonable effort to litigate" is protected "regardless of subjective intent"); *WRTL*, 127 S. Ct. at 2666-67 (opinion of Roberts, C.J., joined by Alito, J.) (test based on subjective intent rejected because it would chill speech by "opening the door" to litigation); *id*. at 2681 (Scalia, J., concurring) (test that is tied to intent is impermissibly vague and would chill speech); *see also* OB 31, 41.

Freedman v. America Online, Inc., 303 F. Supp. 2d 121, 127-28 (D. Conn. 2004), is distinguishable. *Freedman* held that the police could not rely on the emergency exception where the provider did not invoke that provision and the provider's delay in responding suggested that there was no emergency. The *Freedman* court did not address whether the "good faith" standard could be read as embodying an objective standard, or whether such a reading was required in a case implicating constitutional issues. The court was careful to narrow its ruling to the facts. *Id*.

Plaintiffs' other attempts to narrow the emergency exception are unavailing. The exception is not limited to "specific" emergencies, Opp. 7, if by that plaintiffs mean a particular terrorist plot. The possibility that terrorists could launch any of a number of attacks makes the emergency even more serious. Nor does the emergency exception expressly limit the duration of authorized disclosure to emergencies that last only "a few hours or days." Opp. 8. Plaintiffs say that a time limit should be inferred, suggesting that the authorization lasts only as long as it would take to obtain a warrant. *Id*. By definition, however, a limitation that must be inferred is not

clearly and unambiguously required. *INS v. St. Cyr*, 533 U.S. 289, 299 (2001) ("[i]mplications" from statutory text are not a clear statement). Limiting the provider's right to communicate records to circumstances in which the government, in its discretion, chooses to obtain a warrant would constitute an invalid prior restraint. Plaintiffs' suggestion, moreover, is incompatible with the context of ECPA's emergency exception, which is directed at *providers'* authority to disclose information. Because providers cannot obtain a warrant, limiting their authority to act to the time needed for a different party to take action makes no sense. In this respect, Title III's language is not "substantially identical" to ECPA. Opp. 8. Title III authorizes *the government* to intercept calls without a warrant if *the government* determines that an emergency requires interception before an order could be obtained, and *the government* applies for such an order within 48 hours. 18 U.S.C. § 2518(7). By contrast, under ECPA, the provider has no control over whether and how quickly the government may obtain an order. At each point that a provider is evaluating whether to divulge records under this exception, the legal standard is whether such divulgence would reasonably meet an emergency—not how long that emergency has persisted or whether the government had time to obtain a warrant. *In re Application of U.S. for a Nunc Pro Tunc Order*, 352 F. Supp. 2d 45, 47 (D. Mass. 2005), is not to the contrary. Opp. 5 n.6. It held that an order approving past disclosure of records in an emergency was unnecessary because ECPA allows such disclosures without a judicial order. The court said the emergency exception applies when "time is of the essence," *id.*, and because the government claimed that it did not have time to obtain a warrant, the court also mentioned that the emergency exception would apply when there was no time to obtain a warrant—but it did not state that an emergency was limited to that time.

Finally, plaintiffs' position on the emergency exception runs headlong into state secrets. If the alleged records program existed, plaintiffs' erroneous contentions regarding the scope of the emergency exception would require consideration of the nature and imminence of the terrorist threat; defendants' state of mind, which could include what they may have been told by the government when it allegedly requested the records; and the relation between the records and the emergency, which would require delving into the operational details of the alleged records program. If, as plaintiffs claim, these facts are relevant to the applicability of the emergency

exception, the state-secrets privilege would prevent defendants from obtaining and presenting the proof purportedly relevant to rebut plaintiffs' allegations. These are precisely the circumstances in which the state-secrets doctrine requires dismissal. *See infra* at 37-38.

2. *The Rights and Property Exception Applies to the Facts Alleged*

The rights and property exception, 18 U.S.C. § 2702(c)(3), likewise would apply. Its plain language authorizes disclosure when either the provider's "rights" or its "property" are threatened by any source. Fraud (theft of service) is an example, but by no means the only example, of such a threat, and the statutory language is not limited to fraud. Opp. 9-10. Although this exception would not authorize disclosure of a crime wholly unrelated to the provider's operations, *Hodge v. Mountain States Telephone and Telegraph Co.*, 555 F.2d 254, 260 n.16 (9th Cir. 1977), it does permit disclosures when the provider's own rights and property are at risk—and, at a minimum, ECPA does not clearly and unambiguously foreclose that interpretation.

Defendants' alleged communication of records for the purpose of helping the government prevent terrorist attack would fall within the rights and property exception as so construed. First, terrorists threaten to damage defendants' property, as they had done in the 9/11 attacks. Second, defendants had a right to take steps to prevent their property from being used by the enemy, including the right to disclose information to help the government prevent such use. OB 44-45. Plaintiffs do not contend otherwise, resting their argument instead on the broader and erroneous contention that the rights and property exception is limited to theft of service.

The applicability of the rights and property exception, moreover, does not turn on whether a provider communicates records unilaterally or in response to a request from the government. Opp. 10. A provider may not perceive the threat to its property, or know how its records can help prevent such a threat, until the government makes a request. Title III cases are inapposite because when the *content* of communications is intercepted, whatever the scope of the rights and property exception, the Fourth Amendment may come into play. Hence, in some circumstances, "'the requirements of the Fourth Amendment would override [statutory] authority'" to intercept calls. *McClelland v. McGrath*, 31 F. Supp. 2d 616, 619 (N.D. Ill. 1998) (quoting *United States v.*

Pervaz, 118 F.3d 1, 5 (1st Cir. 1997)). This factor does not apply to records. *McClelland* is also inapposite because the court there held only that *the police* could not rely on the rights and property exception; the provider was not sued. *Id*.

V. THE CLAIMS BASED ON THE ALLEGED INTERCEPTION OF CALL CONTENT MUST BE DISMISSED

A. Title III Does Not Apply

FISA, not Title III, applies to surveillance for foreign intelligence purposes. Title III lacks the clear statement required to construe it as applying to the facts alleged. OB 13-14. Section 2511(1) is just the kind of generally-worded prohibition that is not a clear statement. *See* Opp. 11. A reference to "any person," 18 U.S.C. § 2511(1), like a reference to "each authority," *see Franklin*, 505 U.S. at 800-01, cannot be read to apply to the President. Former § 2511(3), OB 7, therefore was not necessary to prevent Title III from applying to the President. Contrary to plaintiffs' suggestion, § 2511(3) neither modified the scope of the prohibition in § 2511(1) nor created an exception to a prohibition that would otherwise reach the President. Rather, § 2511(3) merely confirmed that the scope of § 2511(1)'s prohibition was limited and did not reach national security activities. As the Supreme Court found, former § 2511(3) was "only intended to make clear that the Act simply did not legislate with respect to national security surveillances." *United States v. U.S. Dist. Ct.* ("*Keith*"), 407 U.S. 297, 306 (1972).

When Congress subsequently eliminated this disclaimer in FISA, it did not thereby make a clear statement of intent to extend the prohibition of § 2511(1) to reach foreign intelligence. Even if § 2511(3) had been an exception to § 2511(1), its repeal cannot be read as a clear statement of intent to extend the reach of the prohibition. In *INS v. St. Cyr*, 533 U.S. 289 (2001), the statute at issue had previously provided for judicial review of deportation decisions solely under the Hobbs Act, subject to an exception for habeas review. The government argued that "the inclusion of that exception in [the former] Act indicates that Congress must have believed it would otherwise have withdrawn the pre-existing habeas corpus jurisdiction in deportation cases, and that, as a result, the repeal of that exception … implicitly achieved that result." *Id*. at 309. The Court rejected that argument, finding that the earlier "exception is best explained as merely

confirming the limited scope of the new review procedures," *id*., and in any case "its repeal cannot be sufficient to eliminate what it did not originally grant," i.e., a constitutionally-based right to habeas review, *id*. at 310. The same analysis applies even more strongly to the repeal of § 2511(3), which was merely a "disclaimer" and not an "exception." *Keith*, 407 U.S. at 308.

The structure of Title III and FISA also demonstrates that Congress intended to subject the President's conduct of surveillance for national security purposes solely to FISA, and not to Title III. The whole point of enacting FISA was to regulate foreign intelligence surveillance *in FISA*. OB 7-8. The salient consideration, to which plaintiffs offer no response, is that FISA not only authorizes the President to conduct such surveillance, subject to oversight by a new court, but also establishes its *own* set of prohibitions and remedies for violations. Congress specifically considered *and rejected* a proposal to extend the cause of action in Title III to foreign intelligence surveillance. OB 8 & n.10. The remedies Congress did authorize in FISA, moreover, are different from—and incompatible with—those under Title III. For example, agents of foreign powers cannot sue under FISA, whereas Title III has no such limitation. OB 8-9. In addition, whereas Title III authorizes suits for injunctive and declaratory relief, 18 U.S.C. § 2520(b), such relief is unavailable in the case of foreign intelligence surveillance, 50 U.S.C. § 1810, because it would undermine the exclusive jurisdiction of the FISA courts to authorize surveillance orders, *see ACLU v. Barr*, 952 F.2d 457, 469-71 (D.C. Cir. 1991). The two statutes also authorize different damages awards. *Compare* 18 U.S.C. § 2520(c)(2) (authorizing recovery of profits or statutory damages of up to $10,000), *with* 50 U.S.C. § 1810 (authorizing recovery of statutory damages of up to $1,000 but not profits). Congress thus intended to provide different, and narrower, relief when foreign intelligence surveillance is conducted in violation of FISA than is available under Title III. It is inconceivable that Congress's repeal of § 2511(3)—at the same time that it was creating a comprehensive new regime for foreign intelligence gathering—was meant to subject foreign intelligence surveillance to Title III. As the Ninth Circuit has explained, FISA "is intended to be exclusive in its domain and Title [III] in its." *United States v. Koyomejian*, 970 F.2d 536, 541 (9th Cir. 1992) (en banc) (citation omitted).

Nor do any of the exceptions in Title III demonstrate a clear intent to apply its

prohibitions to the conduct of foreign intelligence surveillance. *See* Opp. 12-14. As noted, an exception cannot be construed as a clear statement of intent to apply the prohibition to the President. *Franklin*, 505 U.S. at 800-01. In addition, the provisions plaintiffs cite are inapposite.

The first clause of 18 U.S.C. § 2511(2)(f) states that Title III, ECPA, and 47 U.S.C. § 605 do not apply to foreign intelligence surveillance *not* regulated by FISA, such as certain calls intercepted outside the U.S. *See* 50 U.S.C. § 1801(f). Because the second clause of § 2511(2)(f) states that the procedures set forth in the enumerated statutes are the "exclusive means" of conducting surveillance or interceptions, the first clause clarifies that this restriction does not apply to the kinds of foreign intelligence surveillance that Congress chose not to regulate. *See* H.R. Rep. No. 95-1283, at 100 (1978) (first clause of § 2511(2)(f) exempts the "acquisition of foreign intelligence information from international or foreign communications by a means other than electronic surveillance, as defined in [FISA]," including "electronic surveillance conducted outside the United States"). The first clause does not suggest, let alone clearly state, that Title III would apply to foreign intelligence surveillance that *is* regulated by FISA.

Title III's safe harbor provisions also are not a clear statement of intent to apply Title III's prohibitions to national security surveillance. Section 2511(2)(e) states that, "[n]otwithstanding any other provision of *this title*"—i.e., all of Title 18—it shall not be unlawful for government employees to conduct foreign intelligence surveillance authorized by FISA. Similarly, § 2511(2)(a)(ii) states that, "[n]otwithstanding *any other law*," private parties may assist those authorized to conduct interceptions under Title III or surveillance under FISA. These provisions do not describe the scope of Title III's prohibition. Instead, they eliminate any argument that conduct that complies with FISA nevertheless could be punished under a variety of other laws. Such confirmatory language does not establish that the laws in question otherwise would apply to foreign intelligence—and certainly does not show clearly that Congress intended to extend Title III into the area of foreign intelligence surveillance that it created FISA to regulate.

B. Plaintiffs Do Not Plead, and Cannot Prove, Acquisition of Calls

Plaintiffs do not assert that any of their calls were selected by computers for human scrutiny or that a computer's alleged scanning of calls constitutes acquisition. Instead, plaintiffs

contend that, before calls are allegedly scanned by a computer, certain technical steps must be taken, such as the redirection of traffic, which they claim constitute acquisition even if calls are not preserved and never heard by a human being. Opp. 19-20. The gravamen of the Complaint, however, is that defendants allegedly gave NSA access to their switches, where the calls were allegedly scanned. *E.g.*, Compl. ¶¶ 145-46. These allegations suggest only that NSA computers purportedly scanned content directly within defendants' networks, without any redirection. The Complaint's use of the legal term "interception" does not suffice. *See supra* at 22.

In any case, plaintiffs cite no case holding that the redirection of traffic for an instant until it is passed through a computer constitutes acquisition. All of the cases plaintiffs cite involve the creation of a recording, which plaintiffs have not alleged. In *Sanders v. Robert Bosch Corp.*, 38 F.3d 736, 739, 742 (4th Cir. 1994), the court distinguished the creation of a tape recording of a call (which it said was an acquisition) from the transmission of sounds from one location to another (which it said was not acquisition if not heard). Redirection of calls without the creation of a recording is no different than the transmission that *Sanders* found was not an acquisition.

In addition, in the Ninth Circuit, even a recording is not an interception if the recording is not heard. *Greenfield v. Kootenai County*, 752 F.2d 1387, 1389 (9th Cir. 1985); *see Arias v. Mut. Cent. Alarm Serv., Inc.*, 202 F.3d 553, 558 (2d Cir. 2000) ("The *Greenfield* court held that telephone calls that were automatically recorded but not listened to were not aurally acquired within the meaning of Title III."). In *Jacobson v. Rose*, 592 F.2d 515 (9th Cir. 1978), the court made clear that the invasion of privacy that Title III prohibits is the act of listening to a call, not merely recording it. "When many individuals together take the steps necessary for the recording of telephone conversations, the victim's privacy is violated, regardless of which particular individuals *actually listen* to the tapes." *Id.* at 522 (emphasis added). A defendant that enabled calls to be recorded was liable "for the invasion of privacy it helped to occasion," *id.*, i.e., the resulting act of listening.[5]

Halkin v. Helms, 598 F.2d 1 (D.C. Cir. 1978), confirms that plaintiffs do not state a claim

[5] Most of the cases plaintiffs cite suggesting that recording constitutes acquisition involve calls that were later heard. Opp. 19 & n.22. The few cases to the contrary are not controlling.

for interception. The *Halkin* plaintiffs claimed that NSA violated Title III by routing a huge volume of communications through computers. *Id.* at 3-4 & n.2. These facts did not make out a claim for interception, absent proof that the plaintiffs' calls were selected by the computers for human examination. *Id*. at 11. Plaintiffs' identical allegations in this case fare no better.

Finally, even under plaintiffs' erroneous view that acquisition occurs whenever traffic is redirected, it would become necessary to determine whether and how traffic was routed to a government computer, and whether any such facts meet plaintiffs' definition of redirection. Any such facts, if they exist, would be shielded by the state-secrets privilege.

C. The FISA Claim Must Be Dismissed

If foreign intelligence surveillance were conducted, as alleged, the only applicable statute would be FISA. Beyond their failure to plead facts establishing surveillance, plaintiffs could not prevail under FISA without evidence protected by the state secrets privilege. For example, to find that FISA validly restricts the President's constitutional authority would require a balancing of the needs of the Executive against those of Congress in the specific factual circumstances. This would require facts about the nature of the terrorist threat and the efficacy of any surveillance program in addressing the threat—facts made unavailable by the state-secrets privilege. OB 11.

VI. THE REMAINING CLAIMS MUST BE DISMISSED

A. Claim 4, Under 47 U.S.C. § 605, Must Be Dismissed

FISA, not 47 U.S.C. § 605, is the statute applicable to surveillance of call content for foreign intelligence purposes. As recognized in *Butenko*, 494 F.2d at 601, § 605 lacks a clear statement of intent to regulate the President's conduct of surveillance to protect the nation from foreign enemies. OB 46. Plaintiffs misread the first clause of 18 U.S.C. § 2511(2)(f). Opp. 13 n.14. As discussed above, that clause simply confirms that § 605 and other provisions do not apply to the interception of calls for foreign intelligence purposes in circumstances *not* regulated by FISA. It does not provide that § 605 applies to foreign intelligence surveillance that *is* regulated by FISA. Congress never clearly expressed its intent for § 605 to regulate the President; the absence of an express "exception" from § 605 for domestic surveillance for foreign intelligence purposes, Opp. 13 n.14, is not such a statement. *See Franklin*, 505 U.S. at 800-01.

For the same reasons, § 605 does not apply to the alleged divulgence of call records for national security purposes. But plaintiffs' records claim under § 605 also fails for another reason: that law does not apply to call records. In *United States v. Barnard*, 490 F.2d 907, 913 (9th Cir. 1973), telephone records were communicated to the government without a subpoena. While the remedy sought was an order excluding the records from evidence, Opp. 13 n.14, the "grounds" for that request were that "the records were disclosed to the government in violation of 47 U.S.C. § 605," 490 F.2d at 913, and the basis for the court's rejection of that argument was that call records "do not fall within the scope of 47 U.S.C. § 605," *id*. That holding is controlling as to the scope of § 605's prohibition. *Brown v. Continental Telephone Co*., 670 F.2d 1364 (4th Cir. 1982), the only case plaintiffs cite, Opp. 13 n.14, is not to the contrary. *Brown* stated that it was "not necessary to consider" whether call records are "protected information within the meaning of the statute." 670 F.2d at 1365. Instead, the court held that a disclosure made in response to a request by the police, unaccompanied by a warrant or court order, was authorized by the provision of § 605 permitting disclosures "on demand of other lawful authority." *Id*. at 1365-66.

B. Claim 1, Under 18 U.S.C. § 2702(a)(1) & (2), Must Be Dismissed

Claim 1, for alleged divulgence of stored content in violation of ECPA, fails for the same reason as the records claim fails: ECPA lacks the clear statement needed to apply it to the President's alleged national security intelligence-gathering activities. Plaintiffs also do not appear to contest the propriety of dismissing this claim in light of their voluntary dismissal of the Verizon entities that provide Internet and e-mail services. OB 46.

C. The State-Law Claims Must Be Dismissed

Because the emergency and rights and property exceptions apply to the facts alleged, plaintiffs' state-law records claims are preempted. ECPA states that "[n]o cause of action shall lie in any court" for actions taken in accordance with "statutory authorization." 18 U.S.C. § 2703(e). ECPA authorizes a provider to disclose records in an emergency and to protect their rights and property. *Id.* § 2702(c)(3) & (4). Hence, any cause of action under state law that is based on conduct falling within those exceptions is barred. The legislative history confirms that Congress included this provision in ECPA for this very purpose. *See* H.R. Rep. No. 107-497, at

16 (2002) (provision "protects providers from law suits when they legally assist law enforcement with an investigation under the new emergency disclosure exception").

In addition, the Constitution precludes plaintiffs' state-law claims. As explained in our opening brief, a fundamental right of citizenship is the ability to communicate information to the Executive for the purpose of protecting public safety. OB 30. This right is inherent in the design of a national government with a direct relationship with the people. *See U.S. Term Limits, Inc. v. Thornton*, 514 U.S. 779, 821 (1995) ("[T]he Framers, in perhaps their most important contribution, conceived of a Federal Government directly responsible to the people, possessed of direct power over the people, and chosen directly, not by States, but by the people."). A "State is not permitted to interpose itself between the people and their National Government." *Cook v. Gralike*, 531 U.S. 510, 527 (2001) (Kennedy, J., concurring). Plaintiffs' attempt to use state law to hold defendants liable for their alleged communications with the federal government violates this basic principle. Whatever the scope of *federal* power to prohibit the communications alleged—and, as shown above, ECPA neither can nor does apply to the facts alleged—state law cannot be applied in any way that would interfere with a citizen's ability to communicate with the federal government. *See U.S. Term Limits*, 514 U.S. at 822 (holding unconstitutional state law that had the purpose and effect of term-limiting the state's congressional delegation because, *inter alia*, permitting states to regulate the qualifications of Members of Congress would "sever the direct link that the Framers found so critical between the National Government and the people of the United States" (footnote omitted)); *Crandall v. Nevada*, 73 U.S. 35, 44 (1867) (in demanding "the services of its citizens ... [the federal government] is entitled to bring them to those points from all quarters of the nation, and no power can exist in a State to obstruct this right").

Plaintiffs' contract and deception claims also fail on their own terms. The privacy policies cited in the Complaint expressly permit disclosures to protect public safety. Plaintiffs do not contest that this language would permit disclosures in the circumstances alleged. OB 47-48. Plaintiffs' conclusory allegation that the privacy policy was breached, Opp. 47, fails in the face of this express language. In addition, the alleged breach of *Verizon's* privacy policy cannot serve as the basis for a claim by plaintiff Landis, who was an MCI customer *before* that company was

acquired by Verizon. OB 47. Assuming the Verizon policy applied to MCI after the acquisition, Opp. 47, the Complaint does not allege facts establishing that this policy became a part of her *contract*. *See Dyer v. Nw. Airlines Corp.*, 334 F. Supp. 2d 1196, 1199-1200 (D.N.D. 2004) (privacy policy does not automatically become a contractual obligation). Plaintiffs suggest that there was a different MCI privacy policy, Opp. 48, but they do not mention it in the Complaint. In fact, the MCI privacy policy is limited to disclosures to third parties for marketing and does not restrict disclosures to the government. *See* Second Request for Judicial Notice, Ex. 1.

VII. THE STATE-SECRETS PRIVILEGE MANDATES DISMISSAL

Plaintiffs' opposition demonstrates that full and fair litigation of the issues that *they* claim would be relevant would require evidence protected by the state-secrets privilege. For example, plaintiffs claim that the emergency and rights and property exceptions are inapplicable because defendants' conduct was unreasonable and was not undertaken in (subjective) good faith. Opp. 5. Plaintiffs contend that these issues involve questions of fact that cannot be resolved on a motion to dismiss. *Id*. As noted, the allegations of the Complaint establish that these exceptions apply as a matter of law. But under plaintiffs' own theory, assuming a records program even exists, these purported factual issues could only be decided with evidence that would bear on reasonableness and subjective good faith—such as what defendants may or may not have been told about the need for and use of the records and how those records may or may not have been used. Similarly, plaintiffs' contention that the records allegedly provided were not of public importance under the First Amendment because they included records of customers with no connection to terrorists (Opp. 34; *see also* Opp. 9 n.10, 40-41) is defeated by the allegations of the Complaint. But if this were deemed a relevant factual issue, it could only be evaluated by obtaining evidence about the degree of relation between the records allegedly divulged and the emergency, including details about the operations of NSA's alleged program. Plaintiffs' brief is littered with other issues of fact that they claim are relevant, such as how the alleged "scanning" of content occurred and whether it involved the creation of a copy or redirection of traffic (Opp. 19-20); whether the alleged disclosures were "in response to specific and urgent emergencies" (Opp. 7); whether and

to what extent NSA analysts had "discretion" to review records allegedly divulged (Opp. 24); the "threat" posed by the government's alleged access to records (Opp. 38); and whether, "as a factual matter," the records allegedly disclosed contain foreign intelligence information (Opp. 16). While none of these factual issues can prevent dismissal, all would be shielded by the state-secrets privilege. *See* Alexander Declaration ¶ 12(c) (Dkt. 254).

As soon as it becomes apparent that evidence necessary to the resolution of the case is rendered unavailable by the state-secrets privilege, dismissal is required. OB 3; Gov't Br. 5. This rule has special force when the state-secrets privilege renders unavailable evidence that would be helpful to the defendant, for it would be fundamentally unfair for the government to subject a defendant to liability while depriving it of any evidence that could be useful in its defense. *Kasza v. Browner*, 133 F.3d 1159, 1166 (9th Cir. 1998); OB 4-5. Plaintiffs' brief highlights this concern. Plaintiffs posit factual issues that they claim must be addressed, even though defendants would be unable to obtain the evidence that plaintiffs say would be necessary to address them. It is now clear not only that plaintiffs would require secrets to make out their prima facie case, but especially that a full and fair defense would be impossible. In these circumstances, it would be both unfair and unnecessary to postpone the inevitable day of reckoning. For these reasons, as well as those presented by the government, which defendants join, the state-secrets doctrine requires immediate dismissal.

VIII. CLAIMS AGAINST MCI ARE BARRED BY THE BANKRUPTCY DISCHARGE

This Court is not the proper forum for resolution of claims against MCI. An outstanding injunction from the Bankruptcy Court requires that plaintiff's claims—which arose prior to MCI's discharge in bankruptcy—be transferred to that court for adjudication.

Plaintiff's main response is that she did not know—and could not have known—about the existence of her claims against MCI at the time of the discharge. Opp. 49-50. But in the Ninth Circuit, a claim arises before discharge if the claimant either (i) had actual or imputed knowledge of the claim, or (ii) had a prior "relationship" to the act or omission that is the subject of the claim. *See In re Jensen*, 995 F.2d 925, 929-30 (9th Cir. 1993); *In re Hassanally*, 208 B.R. 46, 52

(9th Cir. B.A.P. 1997) (*Jensen* fair contemplation test equivalent to the *Piper* prepetition relationship test); *In re Russell*, 193 B.R. 568, 571 (Bankr. S.D. Cal. 1996); *see also In re Piper Aircraft*, 58 F.3d 1573, 1577 (11th Cir. 1995) (citing *Jensen* as recognizing claims "only for those individuals with some type of prepetition relationship with the debtor").

Plaintiff is unable to dispute that she had a pre-discharge relationship with MCI and, further, that her claim arises out of the debtor's alleged pre-discharge conduct. The broad test used in the Ninth Circuit embraces both injuries that are already manifest at the time of the discharge in bankruptcy as well as those that become manifest in the future. In *Piper Aircraft*, a latent defect was not discovered until after the bankruptcy discharge. The court held that because the claimants had a pre-discharge relationship with the manufacturer, parties injured as a result of such a product defect could not pursue the debtor outside of bankruptcy. Their sole recourse was in bankruptcy court. *Piper Aircraft*, 58 F.3d at 1577-78. The same result should obtain here.

Plaintiff also argues that even assuming her pre-discharge claims are barred, her claims related to MCI's post-discharge conduct should nevertheless survive. Opp. 51 (citing *O'Loghlin v. County of Orange*, 229 F.3d 871 (9th Cir. 2000)). But *O'Loghlin* does not change the analysis of when a claim arises in bankruptcy. That case involved three separate decisions by Orange County not to accommodate an employee's disability, one of which was made after the bankruptcy discharge. The Ninth Circuit held that each of the three separate decisions constituted a separate claim and concluded that the County was liable for its post-discharge decision. *Id*. at 875-76. By contrast, plaintiff's allegations turn on the alleged decision by MCI to establish a system to provide NSA access to its call content and records—a decision allegedly made and implemented shortly after 9/11, well before MCI's bankruptcy discharge. Compl. ¶¶ 149, 169-70.

Plaintiff's allegations are unlike those at issue in *O'Loghlin*, but are indistinguishable from the claims for permanent trespass based on MCI's installation of fiber-optic cable on land allegedly owned by others. Those trespass claims arose pre-discharge, even though the challenged action has post-discharge effects. *In re WorldCom, Inc.*, 320 B.R. 772, 782-83 (Bankr. S.D.N.Y. 2005); *In re WorldCom, Inc.*, 328 B.R. 35, 57-58 (Bankr. S.D.N.Y. 2005). In *West v. WorldCom, Inc.*, 2007 WL 485233 (S.D.N.Y. Feb. 13, 2007), the court affirmed the latter

decision insofar as it held that a claim based on permanent trespass, occasioned by the installation of cable, arose pre-discharge. *Id*. at *3. *West* reversed the Bankruptcy Court only to the extent that the District Court deemed MCI's post-petition maintenance a separate tort and not part of the permanent trespass. *Id*. at *3-4. Plaintiff does not allege such facts.

The question posed by plaintiff's allegations—when does a "claim" arise for purposes of bankruptcy law—also highlights why the state-secrets privilege would prevent defendants from fully and fairly litigating this case. To the extent that issue could not be resolved based on the facts pled, it would be necessary to delve into operational details about the alleged system that NSA purportedly relied on to extract information from MCI, including how, when, and where the alleged system was established, and the means by which the information allegedly is extracted.

Lastly, plaintiff relies on two inapposite procedural arguments. First, plaintiff complains that she did not receive actual notice of the MCI bankruptcy. Opp. 49. As in *Piper Aircraft*, however, the pre-discharge relationship and the constitutionally adequate publication notice are sufficient to satisfy due process. MCI fulfilled its due process obligations to all potential and future claimants—including Landis—by an extensive regime of publication notice. *See Mullane v. Cent. Hanover Bank & Trust Co.*, 339 U.S. 306, 317 (1950); *Monster Content, LLC v. HOMES.COM, Inc.*, 331 B.R. 438, 442 (N.D. Cal. 2005). Second, plaintiff incorrectly asserts that the Federal Rules of Civil Procedure prohibit Verizon from raising the issue of discharge in a motion to dismiss. Rule 8(c) provides that "[i]n pleading to a preceding pleading, a party shall set forth affirmatively . . . discharge in bankruptcy . . . ." Fed. R. Civ. P. 8(c). A motion to dismiss is not a "pleading" for purposes of Rule 8, and thus a defendant may raise the affirmative defenses listed in Rule 8 in a motion to dismiss without waiving that defense. *See Morrison v. Mahoney*, 399 F.3d 1042, 1046-47 (9th Cir. 2005).

IX. CONCLUSION

For these reasons and those in our opening brief, defendants' motion should be granted.

Dated: August 3, 2007

WILMER CUTLER PICKERING HALE AND DORR LLP

MUNGER, TOLLES & OLSON LLP

Randal S. Milch

By: /s/ John A. Rogovin

John A. Rogovin

Attorneys for Verizon Communications Inc., Verizon Northwest Inc., Verizon Florida Inc., and MCI Communications Services, Inc.