Nos. 06-17132, 06-17137

IN THE UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

TASH HEPTING, *et al.*,
Plaintiffs/Appellees,

v.

AT&T CORP.,
Defendant/Appellant.

TASH HEPTING, *et al.*,
Plaintiffs/Appellees,

v.

United States,
Defendant-Intervenor/Appellant.

On Appeal from the United States District Court
for the Northern District of California

BRIEF OF *AMICUS CURIAE* VERIZON COMMUNICATIONS INC. IN SUPPORT OF AT&T CORP. AND THE UNITED STATES

Henry Weissmann
MUNGER, TOLLES & OLSON LLP
355 South Grand Avenue, 35th Floor
Los Angeles, CA 90071-1560
(213) 683-9100

John A. Rogovin
Randolph D. Moss
Samir C. Jain
WILMER CUTLER PICKERING
HALE AND DORR LLP
1875 Pennsylvania Avenue, NW
Washington, DC 20006
(202) 663-6000

March 20, 2007

Attorneys for Verizon Communications Inc.

CORPORATE DISCLOSURE STATEMENT

Pursuant to Rule 26.1 of the Federal Rules of Appellate Procedure and Circuit Rule 26.1-1, Verizon Communications Inc. submits the following corporate disclosure statement:

Verizon Communications Inc. is a publicly held corporation that owns the following subsidiaries having securities in the hands of the public:

Verizon Delaware LLC.
[formerly known as "Bell Atlantic - Delaware, Inc." and "The Diamond State Telephone Company"]

Verizon Maryland Inc.
[formerly known as "Bell Atlantic - Maryland, Inc." and "The Chesapeake and Potomac Telephone Company of Maryland"]

Verizon New Jersey Inc.
[formerly known as "Bell Atlantic - New Jersey, Inc." and "New Jersey Bell Telephone Company"]

Verizon Pennsylvania Inc.
[formerly known as "Bell Atlantic - Pennsylvania, Inc." and "The Bell Telephone Company of Pennsylvania"]

Verizon Virginia Inc.
[formerly known as "Bell Atlantic - Virginia, Inc." and "The Chesapeake and Potomac Telephone Company of Virginia"]

Verizon West Virginia Inc.
[formerly known as "Bell Atlantic - West Virginia, Inc." and "The Chesapeake and Potomac Telephone Company of West Virginia, Inc."]

Verizon New York Inc.

[formerly known as "New York Telephone Company"]

Verizon New England Inc.

[formerly known as "New England Telephone and Telegraph Company"]

Verizon California Inc.

[formerly known as "GTE California Incorporated"]

Verizon Florida LLC.

[formerly known as "GTE Florida Incorporated"]

Verizon North Inc.

[formerly known as "GTE North Incorporated"]

Verizon Northwest Inc.

[formerly known as "GTE Northwest Incorporated"]

Verizon South Inc.

[formerly known as "GTE South Incorporated"]

Verizon Capital Corp.

Cellco Partnership (dba "Verizon Wireless")

NYNEX Corporation

GTE Corporation

GTE Southwest Incorporated (dba Verizon Southwest)

In addition, Verizon Communications Inc. owns a 52% interest in Telecommunicaciones de Puerto Rico, Inc., which has publicly traded notes. Verizon also owns non-controlling minority interests in various companies that have publicly held securities.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Federal Cases

Federal Statutes

Rules

INTEREST OF *AMICUS CURIAE*

The *Hepting* case is now part of a consolidated multidistrict litigation ("MDL") pending before the Honorable Vaughn R. Walker in the Northern District of California. Among the cases pending alongside *Hepting* in the MDL are more than 20 class actions against Verizon Communications Inc. and its affiliates ("Verizon"). Those suits make essentially the same claim against Verizon that plaintiffs here make against AT&T: that, in the wake of the 9/11 terrorist attacks, Verizon gave the National Security Agency ("NSA") access to the contents of customers' communications and call records without lawful authorization as part of an NSA counter-terrorism program. The central issue in this appeal—whether the government's state-secrets assertion prevents the litigation of plaintiffs' claims—is therefore of critical importance to Verizon.

Pursuant to Federal Rule of Appellate Procedure 29, Verizon submits this amicus brief in support of the United States and AT&T with the consent of all parties to this appeal.

ARGUMENT

I. THE DISTRICT COURT ERRED IN FAILING TO CONDUCT A PROSPECTIVE EVALUATION

Whenever the government asserts the state-secrets privilege as to certain matters, the court has an obligation to assess how the absence of those matters will affect the parties' ability to litigate the case. The central inquiry is this: Without those matters in evidence, *can the case (or a claim) be fully and fairly litigated to completion*? As soon as it becomes apparent that it cannot be, the case or claim must be dismissed.

This essential inquiry requires the court to look ahead—to make a ***prospective*** evaluation. The court must evaluate how the unavailability of secret matter would ultimately impact both (a) plaintiffs' ability to meet jurisdictional requirements (such as standing), prove all elements of their claim, and show entitlement to relief; and (b) defendants' ability to dispute those claims and advance all arguments and defenses with full force. If, looking down the road, it is apparent that the absence of secret matter will compromise either party's ability to litigate the case fully and fairly, dismissal is required.

The fundamental problem in this case is that the District Court did not make this forward-looking assessment. A court's task, before continuing down the road, is to look ahead to see whether there are roadblocks that will prevent completion of the journey. The District Court, however, did not come to grips with the clear

roadblocks in this case. Instead, the court's approach was to look only at the pavement in front, and to wade into a host of sensitive issues, before coming to the inevitable dead-end. There may be cases where pushing forward is appropriate. But *that* judgment can only be made by *undertaking* the necessary prospective analysis and determining that (a) the case likely can be completely litigated without disclosing state secrets, and (b) the incremental steps being taken will likely arrive at that result. This approach might be appropriate, for example, in a lawsuit that deals primarily with public matters and touches only peripherally on a classified item. In such cases, it may be possible to finesse privilege obstacles by exploring the feasibility of a "workaround"—allowing discovery, for example, to establish an alternative, non-secret means of proof. *See United States v. Reynolds*, 345 U.S. 1, 11 (1953).

But this is not such a case. This case is *all about* secret subject matter: Plaintiffs challenge the legality of alleged intelligence activities that are secret, whether their general existence is acknowledged or not. The very "stuff" of this case is secret activities. The required evaluation shows that this case cannot be litigated to conclusion, and indeed (as the government and AT&T have shown) standing cannot be established. The state-secrets issues can neither be finessed nor evaded.

A. The Nature of the Required Inquiry

When a suit concerns secret matters, the required prospective analysis proceeds in two stages. The first question is whether the suit falls into one of two categories of cases identified by the Supreme Court as requiring outright dismissal—without the need for any granular analysis—because of the nature of the claims involved. Cases falling within these categories must be dismissed because the substance of the claims inherently precludes litigation. These cases are: (1) those whose "very subject matter" are secret, and/or (2) those which would involve courts in exposing, probing, or betraying relationships between the Executive and private parties who have agreed to collect intelligence for national defense. If either of these categorical rules applies, the case must be dismissed right away. If not, then the court must perform the forward-looking analysis of whether the case can be fully litigated without state secrets. This involves an assessment of whether, as the case will eventually play out, plaintiffs would be required to rely on facts that are a state secret, or defendants could be deprived of evidence that might be relevant to their defense. If any of these tests is met, the case must be dismissed.

1. The parameters of the first categorical bar to litigation—cases whose "very subject matter" is secret—are clear. These are suits where the substance of the claim necessarily would require disclosure of secret matters. Some cases fall

into this category because the existence of the activity they seek to challenge is secret. *See, e.g., Kasza v. Browner*, 133 F.3d 1159, 1170 (9th Cir. 1998). In other cases, the existence of a program may have been acknowledged in general terms, but the operational details and activities involved in the program remain secret. *See El-Masri v. United States*, 2007 WL 625130, at *8 (4th Cir. Mar. 2, 2007). A case that challenges the legality of such a program cannot be fully and fairly litigated because the whole focus of the case is the secret subject matter. The relevant facts are either secret, or so entangled with secrets, that either the plaintiffs will be unable to establish their claims, or the defendant will be unable to mount a full defense, or both. As the Fourth Circuit recently noted, even where the existence of a program is acknowledged in general terms, dismissal is still required where it is apparent that the litigation will involve exposing operational details, activities, and information that remain secret. *Id.*

State-secret barriers often proliferate when plaintiffs, instead of suing the government, choose to challenge a program by suing a private party allegedly cooperating in the program. Many such suits have not only all the same problems that exist in suits against the government, but a whole additional layer as well. Plaintiffs cannot win just by showing that the *government* had a program: They must also show that the *private party* participated with the government in carrying out the program. This would necessarily involve probing and exposing an

intelligence relationship between the government and a private party. Just as critically, plaintiffs must do more than show someone "cooperated" with the government: They must show that the specific actions taken by a private party violated specific prohibitions in federal statutes. Thus, these cases tend to threaten greater intrusion into the specific details of intelligence collection methods and activities than do suits against the government alone. *See Farnsworth Cannon, Inc. v. Grimes*, 635 F.2d 268, 281 (4th Cir. 1980) (en banc) (per curiam).

2. In cases like this, another categorical rule applies. The *Totten* doctrine bars all litigation that would expose, probe, or betray a confidential relationship the President has entered into with a private party to collect intelligence on behalf of the government. *See Totten v. United States*, 92 U.S. 105, 107 (1875); *see also Tenet v. Doe*, 544 U.S. 1, 11 (2005). These cases have frequently arisen where the private agent himself is seeking to litigate against the government, but the Supreme Court has made clear that the rule's purpose applies with equal force to cases where a stranger to the relationship seeks to expose it. As the Court explained in *Totten*, the purpose of the rule is to protect the confidentiality of intelligence service on behalf of the government for national defense purposes "where a disclosure of the service might compromise or embarrass our government in its public duties, or endanger the person or injure the character of the agent." 92 U.S. at 106. The rule is based on recognition that the

President must be able to enlist private parties to carry out his constitutional responsibilities for collecting intelligence, and if litigation is allowed to invade those relationships, the President's ability to obtain help would soon evaporate and, with it, his effectiveness in protecting the country. *See id.* at 107 (noting that "secret service, with liability to publicity in this way, would be impossible"); *see also Weinberger v. Catholic Action of Hawaii/Peace Educ. Project*, 454 U.S. 139, 146-47 (1981) (relying on *Totten* to dismiss claim by plaintiff who was not party to the alleged secret relationship); *El-Masri*, 2007 WL 625130, at *8 (relying on *Totten* to dismiss claim against private defendants by plaintiff who was not party to the alleged secret relationship).

3. Finally, if and only if neither of the foregoing categorical rules applies, a court must engage in the forward-looking analysis to determine whether the issues presented in the litigation of a claim would involve state secrets. For example, if establishing the elements of a prima facie claim requires a plaintiff to use state secrets, the case must be dismissed at the outset. *See Kasza*, 133 F.3d at 1166. But the court must also consider the impact of state secrets on the defendant. *Id.* A defendant cannot be forced to give up any facts that may strengthen its defense. The court must consider not simply whether state secrets will deprive a defendant of a defense entirely, but whether the defendant could present its defense more fully if secrets were used to support it. If so, the state-secrets doctrine

mandates dismissal, for it would violate fundamental due process for the government to subject a defendant to liability and at the same time deprive it of evidence that could be useful in its defense. *See Philip Morris USA v. Williams*, 127 S. Ct. 1057, 1063 (2007) (Due Process Clause prohibits "punishing an individual without first providing that individual with an opportunity to present every available defense" (citation and internal quotation marks omitted)).

The District Court failed to make the prospective analysis required by these principles. As to the claims based on the alleged disclosure of records, even though the District Court acknowledged that the existence of that alleged program, and any persons who may be associated with it, have never been acknowledged, the court refused to apply the "subject matter" bar or the *Totten* bar to dismiss the case. (*See* II.A., *infra*.) As to the claims based on the alleged interception of the content of calls, the court truncated the "subject matter" analysis and overrode the *Totten* bar. (*See* III.A., *infra*.) After passing over the categorical bars, the court failed to engage in any prospective evaluation of whether or how the parties could possibly litigate the case to completion without intruding into state secrets. Instead, the court concluded that it was "premature" to determine whether state secrets would prevent the introduction of relevant evidence. *Hepting v. AT&T*, 439 F. Supp. 2d 974, 994 (N.D. Cal. 2006).

B. Deferring the Prospective Inquiry Subverts the Purpose of the Doctrine

The state-secrets doctrine does not allow a court to ignore foreseeable bars to litigation and to continue the litigation until state secrets make it impossible to go farther. Deferring the resolution of whether state secrets would eventually preclude the complete litigation of the case subverts the very purpose of the state-secret privilege.

First, deferral creates wholly avoidable conflicts between the courts and the Executive over secrecy issues. Resolution of state-secret issues involves sensitive separation-of-powers issues between the Judiciary and the Executive. *See El-Masri*, 2007 WL 625130, at *4 (state-secrets doctrine "performs a function of constitutional significance, because it allows the executive branch to protect information whose secrecy is necessary to its military and foreign-affairs responsibilities"); *see also id.* (collecting cases). This separation-of-powers concern calls for sequencing decisions in a way that minimizes conflicts. If foresight would indicate that fact "Z" is a secret whose unavailability will ultimately preclude the resolution of the case, then it creates unnecessary and prolonged battles with the Executive for the court and parties to litigate whether facts "A" through "Y" require protection as state secrets as well. If, by looking ahead, one can see the case cannot be resolved without running into state secrets, it makes no sense to plow through a host of sensitive issues until reaching the

inevitable dead-end. This is an application of the broader principle that courts should avoid delicate constitutional issues. *See Christopher v. Harbury*, 536 U.S. 403, 417 (2002) (in a case touching on the Executive's foreign affairs powers, "the trial court should be in a position as soon as possible in the litigation to know whether a potential constitutional ruling may be obviated" because the complaint fails to state a claim).

The District Court's mode of proceeding will engender needless conflict with the Executive. It is apparent now that plaintiffs cannot prove that they have standing to challenge the Terrorist Surveillance Program ("TSP")[1] because the facts as to whose transnational calls were or were not intercepted are secret. At the end of the day, the court's judicial power over that claim cannot be established. Nonetheless, the District Court kept the claim alive, deferring the substance of the standing problem by dealing with it as a pleading matter at the earliest stage of litigation. But it is wrong for a court to override the government's secrecy judgments and compel disclosure of the identity of the companies that allegedly supported the program where it is clear at the outset that the court's jurisdiction cannot be established. *See Halkin v. Helms*, 690 F.2d 977, 998 (D.C. Cir. 1982)

---

[1] As AT&T has explained, *see* Br. of Appellant AT&T Corp. 7-10, the District Court erred in eliding the crucial distinction between the TSP acknowledged by the President and the broader contents "dragnet" that plaintiffs allege. In this brief, however, Verizon will explain that the court's reasoning was flawed even on its own terms, irrespective of the TSP-dragnet distinction.

("the impossibility of proving that interception of any appellant's communications ever occurred renders the inquiry pointless from the outset"); *see also id.* at 999.

Litigation of this case is precluded whether or not the plaintiffs' calls were *in fact* intercepted because those facts cannot be established without disclosure of secrets. Suppose that, in a case like this, the court were to review in camera whether any plaintiffs' calls were in fact intercepted. If, after that review, it proceeded with the case, the court would be implying that the plaintiffs' calls *were* intercepted—a secret fact. The alternative explanation—that the court would allow the case to proceed even though it knew that the plaintiffs' calls were not in fact intercepted—would be alarming. In that case, it would be clear that plaintiffs lack standing and that the court lacked judicial power over their claims. In these circumstances, it would be improper for a court to continue with the case, forcing the government to defend its claims of state secrets with respect to matters unrelated to standing and forcing defendants to endure protracted litigation over claims as to which the court lacks jurisdiction. As then-Judge Scalia stated in upholding the dismissal of a "refusal-to-hire" case on state-secrets grounds:

> As a result of that [in camera review] process, the court knows that the reason [plaintiff] was not hired [by the FBI] had nothing to do with [his father's] assertion of First Amendment rights. Although there may be enough circumstantial evidence to permit a jury to come to that erroneous conclusion, it would be a *mockery of justice* for the court—knowing the erroneousness—to participate in that exercise.

Molerio v FBI, 749 F.2d 815, 825 (D.C. Cir. 1984) (emphasis added).

The second problem with the District Court's approach is that the very *process* of litigation threatens the improvident disclosure of secrets. The process of discovery (which the District Court appears ready to authorize, 439 F. Supp. 2d at 994); the probing by plaintiffs; the briefing, argument, and submissions (in camera and public) on each incremental decision; the process of handling evidence and witnesses; further interlocutory appeals—at every step of the way, there is a real danger of compromising secret information. *See Farnsworth Cannon*, 635 F.2d at 281. This danger is magnified to the extent the District Court effectively compels the government to disclose secret information in camera in order to protect it—a procedure that the Supreme Court has disapproved. *See United States v. Reynolds*, 345 U.S. 1, 10 (1953). These risks should not be run when the case is fated to ultimate dismissal. "Courts are not required to play with fire and chance further disclosure—inadvertent, mistaken, or even intentional—that would defeat the very purpose for which the privilege exists." *Sterling v. Tenet*, 416 F.3d 338, 344 (4th Cir. 2005). The District Court seemed to acknowledge a similar risk, noting the possibility that the government or the defendants "might disclose, either deliberately or accidentally, other pertinent information about the communications records program as this litigation proceeds." 439 F. Supp. 2d at 997. The possibility of a leak of classified information, however, is a reason to dismiss the

case now on the basis of state secrets, not (as the District Court believed) a reason to keep the case alive.

Third, deferring resolution of the government's claim of state secrets despite a foreseeable inability to litigate the case fully and fairly to conclusion unfairly prejudices the private defendant. Plaintiffs have made sensationalistic claims of dragnet interception—which the District Court construed as alleging that every call in the United States was intercepted, 439 F. Supp. 2d at 1001—and seek massive statutory damages with no showing of actual harm. AT&T is a widely held public company. Ordinarily, it would be able to defend itself against such accusations publicly, explaining either that it did not participate or that any participation was fully justified, reasonable, and lawful, thus assuaging concerns among customers and investors. Where a defendant is silenced by the government's privilege, it is incumbent on the courts to ensure that the litigation is not unnecessarily prolonged. Protracted litigation that accuses a company of cooperating with the government, amplified by judicial speculation about the existence of such a relationship, presents palpable risks.

As this Court has recognized, application of the state-secrets privilege in cases in which plaintiffs have otherwise valid claims can be harsh, but the "greater public good" and "ultimately the less harsh remedy" is the protection of national security. *Kasza*, 133 F.3d at 1167 (citation and internal quotations omitted). Even

apart from whether plaintiffs in this case have valid claims, dismissal of this case is a less harsh result than it might typically be. Unlike cases such as *El-Masri*, in which the state-secrets privilege barred claims by a plaintiff who had alleged tangible injury, plaintiffs in this case have not alleged actual damage. More fundamentally, the proper forum for consideration of the activities alleged is the political branches, which are actively examining these issues. Appropriate committees of Congress are involved and the Attorney General has stated that the TSP is now being conducted pursuant to court order.

II. THE RECORDS CLAIMS ARE BARRED BY THE STATE-SECRETS DOCTRINE

The District Court found, as to plaintiffs' call records claim, that: (1) unlike the TSP, the government had never acknowledged even the existence of a records program and regarded that issue as a secret; (2) apart from whether it existed, the government had never disclosed which, if any, private companies may have had a relationship to such a program; and (3) apart from whether it existed, the government had not disclosed even the general contours of any such program, much less any operational details. 439 F. Supp. 2d at 997.

Yet rather than making the required prospective assessment whether such a case could be litigated fully and fairly to conclusion, the Court refused to dismiss the case, stating only that it was "hesitant to conclude" that the mere fact whether a program existed or not constituted a state secret. *Id.* The Court noted that, if the

case were kept pending, the government or the defendant might "deliberately or accidentally" disclose information about a records program, thus revealing some secrets. *Id.* at 997-98. This approach contravened the Court's obligation under the state-secrets doctrine.

1. Initially, apart from whether the existence of an alleged records program is secret, the claim against AT&T is categorically barred under the *Totten* doctrine. As noted, *Totten* precludes litigation that exposes or probes spying relationships between the Executive and private parties. That is the essence of plaintiffs' records claim: Plaintiffs must show not only "a" program exists, but also that AT&T was involved in the program in a way that was actionable. The government has never acknowledged any such relationship with AT&T or disclosed the identity of any company that might have entered into any such alleged intelligence collection relationship. Plaintiffs must force the disclosure of these facts, exposing and probing any relationship that AT&T had to the alleged program. This inquiry is categorically barred by the *Totten* doctrine. Even if AT&T were publicly to acknowledge its role in a clandestine government program (which it has not done), the *Totten* doctrine would bar the action. Only the government can waive the *Totten* privilege. *Reynolds*, 345 U.S. at 7. In *Totten*, 92 U.S. at 107, and in *Tenet v. Doe*, 544 U.S. at 11, a self-styled spy's acknowledgment of his relationship to the government was insufficient to defeat

the privilege. Unless and until the government itself formally acknowledges its secret relationship to a private party, litigation either exposing or delving into the relationship is impermissible, regardless of what private parties say or do. The District Court's hesitancy about whether the mere existence of "a" program should be secret has no bearing on whether litigation exposing AT&T's alleged role can be permitted to proceed.

The District Court's reasoning did not come to grips with the *Totten* bar. After initially casting the question as whether the mere existence of "a" program should be secret, the District Court then immediately converted that into a very different question—whether any role of AT&T's should be secret. The court then embarked on a tentative analysis of whether exposure of AT&T's role could really harm the alleged program. But the application of *Totten* does not depend on showing that exposure of a spying relationship would actually harm *the particular program*. The rule of *Totten* is categorical: As a category, spying relationships are to be treated as per se legitimate state secrets. The Supreme Court has made plain that the relationships are protected not because exposure will harm any specific program—after all, *Totten* arose many years after the Civil War—but to avoid either compromising the Executive's intelligence functions in a broader sense, or harming those agents willing to assist. In short, the court's stated reason for refusing to dismiss the record claims could not justify avoiding *Totten*'s bar.

2. Dismissal of the records claims was also required because their "very subject matter" is a state secret. As noted, the "subject matter" bar applies whenever the substance of the claim necessarily would require disclosure of secret matters and it is apparent that the claim could not be fully and fairly litigated to completion. Plaintiffs' records claim runs headlong into this categorical rule. Plaintiffs' case is barred because it challenges the legality of an alleged program that the government has never acknowledged. And even if the general existence of a records program had been acknowledged, plaintiffs would still need to prove that the specific activities allegedly undertaken by the government and AT&T in such a program were unlawful. Again, because the government has never revealed such operational details, litigation challenging the lawfulness of those activities is categorically barred. *See El Masri*, 2007 WL 625130, at *9. Rather than keep this litigation alive based on the possibility that information might be revealed that could enable the case to proceed, the District Court should have dismissed this case based on the government's assertion that any facts pertaining to the alleged records program are secret.

3. But even if this case were not barred by these categorical rules, the District Court was still obligated to make the prospective inquiry as to whether the case could be fully litigated without intruding on state secrets. Complete litigation of plaintiffs' claims is impossible. Secrets loom at every turn. This case is all

about the precise nature of the alleged *secret* records program and the precise nature of AT&T's alleged *secret* involvement. Plaintiffs could not establish their claim, and defendants could not mount a full defense, in the absence of state secrets. A few examples suffice:

The essence of the claim is that NSA developed a secret intelligence capability through which it was able to correlate records of phone calls with other sources of information to detect terrorists. The Complaint alleges that call record information about plaintiffs was placed in a secret database to which NSA was given some kind of "access." *Hepting v. AT&T Corp.*, No. C-06-0672 (N.D. Cal.), Am. Compl. ¶ 51. Assuming the truth of these allegations, any information about what records were contained in such a database, how they were accessed, and the results of any searches of those records reveals the extent of this intelligence capability. Such revelations would be inevitable as plaintiffs seek to make out a prima facie case that AT&T violated the Electronic Communications Privacy Act ("ECPA"), which states that a provider may not "divulge" a record or other information pertaining to a subscriber to a government entity. 18 U.S.C. § 2702(a)(3). Initially, plaintiffs would need to establish whether such databases existed and whether and to what extent they contained records "pertaining to" plaintiffs. This would require plaintiffs to obtain evidence regarding the nature of

the database and whether the information it contains identifies particular subscribers.[2]

In addition, because this is a nationwide class action, the facts sought would necessarily disclose the full scope of the data to which NSA was allegedly given access, which would reveal any temporal, geographic, or other gaps or limitations in the database that could be of value to terrorist enemies. Moreover, to establish whether any record was "divulged," plaintiffs would need to obtain evidence about precisely how NSA obtained any records, including the physical facilities involved; the predicate for accessing the records; the computer algorithms used to search the records; whether NSA used computer searches exclusively or also authorized human inspection; and, if the latter, under what circumstances. Finally, to establish damages, plaintiffs would have to ascertain who within NSA obtained records pertaining to any of the plaintiffs and how those individuals used that information. Any information pertinent to these issues would involve sensitive details regarding intelligence sources and methods and the functioning of an intelligence capability.

---

[2] Notably, the Amended Complaint, ¶ 53, alleges that the database tracks telephone numbers and call duration, but says nothing about whether the database also correlates those numbers to subscriber's names. Another pending complaint alleges that the government can determine subscriber identity by matching the numbers with other databases. *See Riordan v. Verizon Commc'ns, Inc.*, No. 06-3574 (N.D. Cal.), Compl. ¶ 2. If these allegations are true, plaintiffs would have to determine whether and under what circumstances customer numbers are matched with customer names.

If a records program existed, and if AT&T was involved, it would become necessary also to consider whether AT&T's actions were authorized by ECPA's emergency exception, which permits a provider to divulge records to the government "if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of information relating to the emergency." 18 U.S.C. § 2702(c)(4). If AT&T was involved in a secret records program, it would be entitled to present any and all evidence relevant to the applicability of the emergency provision, including information about the gravity of the terrorist threat, its exigent nature, the past and prospective usefulness of the call record information in detecting and preventing terrorist attacks, the inadequacy of other means available to NSA to obtain such information, and what AT&T was told about the foregoing by the government or learned through its participation in the secret program. These matters are and must remain secret.

III. THE CONTENTS CLAIMS ARE BARRED BY THE STATE-SECRETS DOCTRINE

The District Court likewise misapplied the state-secrets doctrine to plaintiffs' content-interception claims.

1. The content claims are clearly barred by the *Totten* doctrine. The District Court found *Totten* inapplicable for two reasons. The court first suggested that *Totten* applies only when the plaintiff is the spy. 439 F. Supp. 2d at 991. As

noted, however, the Supreme Court has made clear that the rule is based not simply on a bargain between the spy and the government but reflects a much broader purpose, namely, to protect the ability of the President to recruit private parties for clandestine relationships and the consequent need to avoid harm to those who enlist to aid the government. *See Totten*, 92 U.S. at 106. Moreover, the Court has relied on *Totten* to bar a stranger's claim against the government. *See Weinberger*, 454 U.S. at 146-47. Thus, there can be no doubt that the *Totten* rule is predicated *not* on a contractual duty but on the *secrecy* of the subject matter, i.e., the relationship.

Next, and "[m]ore importantly," the District Court rejected the *Totten* privilege on the ground that the existence of a secret relationship between AT&T and the government had been "for all practical purposes already disclosed" by the government and AT&T. 439 F. Supp. 2d at 991-92. This conclusion was both inapposite and incorrect. Even if AT&T had admitted its involvement in the TSP—and, as AT&T's brief at 38-43 ably demonstrates, it made no such admission—any statements by AT&T are irrelevant to the applicability of the *Totten* doctrine. "The privilege belongs to the Government and … can neither be claimed *nor waived* by a private party." *Reynolds*, 345 U.S. at 7 (emphasis added). In fact, as the District Court notes, in *Totten* itself the action was brought by a self-proclaimed spy, yet the spy's unmistakable disclosure of the existence of a secret

relationship did not vitiate the applicability of the *government's* privilege. *See also Tenet v. Doe*, 544 U.S. at 11. If a spy's express public disclosure of his status does not undermine the government's privilege, AT&T's broad statements about its general disposition to help the government plainly cannot do so either. Only the government can waive the *Totten* privilege, and it has not done so in this case. On the contrary, the government has never identified which telecommunications carriers, if any, participated in the TSP.

The District Court nevertheless speculated that AT&T may have been involved in the TSP because of its size and ubiquity. 439 F. Supp. 2d at 992. But *Totten*'s applicability depends not on whether the judiciary can surmise that a clandestine relationship may have existed, but rather on whether the Executive has formally asserted that any such relationship is secret. A major purpose of the *Totten* doctrine is to prevent litigation that would confirm or disprove the existence of such suspected relationships. On the basis of its finding that it was "unclear" whether the TSP could have existed without AT&T's participation, *id.*, the District Court set in motion a litigation process that, following discovery, will culminate in a factual finding as to whether and in what ways AT&T was involved in the secret program. This is the essence of what the *Totten* doctrine shields from disclosure. But beyond establishing the ***existence*** *vel non* of a clandestine relationship between AT&T and the government, further litigation will result in probing the ***nature*** of

any such relationship. All the District Court was able to hypothesize was that the TSP may have required AT&T's "acquiescence and cooperation." *Id.* But to establish liability, plaintiffs will have to determine exactly what actions AT&T took. *Totten* shields from judicial examination not only the identity of spies, but also their secret work.

2. The content claims also should be dismissed because their very subject matter is secret. The District Court arrived at a contrary conclusion because the government had made public the existence of "some kind of surveillance program." 439 F. Supp. 2d at 994. But that is only the start of the required inquiry. While the government has described "the general contours" of the TSP, *id.* at 997, it has not publicly disclosed the specific activities taken to implement that program. A challenge to the legality *of those actions* cannot be pursued without revealing secret information about how the TSP has been conducted. Because the very subject matter of the suit is the legality of secret activities, the case is categorically barred by the state-secrets doctrine.

The Fourth Circuit's decision in *El-Masri*, handed down after the District Court's decision in this case, is on point. Just as the existence of "some kind of surveillance program" is known, so too the existence of some kind of CIA rendition program was known. But "[t]he controlling inquiry is not whether the general subject matter of an action can be described without resort to state secrets.

Rather, we must ascertain whether an action can be *litigated* without threatening the disclosure of such state secrets." *El-Masri*, 2007 WL 625130, at *8 (emphasis in original). Although Mr. El-Masri's alleged detention and interrogation had been publicized, litigation of his claims would have required evidence of "the roles, if any, that the defendants played in the events [plaintiff] alleges," which would involve "evidence that exposes how the CIA organizes, staffs, and supervises its most sensitive intelligence operations," including how the CIA obtains assistance from private companies under secret contracts. *Id.* at *9. Because these operational details of the rendition program had never been disclosed, the action was barred by the state-secrets doctrine. Likewise, the operational details of the TSP, and the relationship of any private parties to it, are secret, and litigation challenging those activities as unlawful is categorically barred.

3. In addition to these categorical bars, the case should be dismissed because the claims cannot be proven, or defenses presented fully and fairly, without secret information. To establish a prima facie case of a violation of Title III, plaintiffs must demonstrate that their calls were "intercept[ed]." 18 U.S.C. § 2511(1). An "intercept" means the "acquisition" of the contents of a call through the use of a "device." 18 U.S.C. § 2510(4). To establish a claim under the Foreign Intelligence Surveillance Act ("FISA"), 50 U.S.C. § 1810, plaintiffs must prove, among other things, "electronic surveillance," § 1809, which means the

"acquisition" of the contents of a call, *id.*, § 1801(f). These laws require a plaintiff to prove, at a minimum, that his or her calls were actually acquired. That fact itself is a state secret. *Halkin v. Helms*, 598 F.2d 1, 8 (D.C. Cir. 1978). But beyond the *fact* of acquisition of the content of a particular call, plaintiffs would also need to prove the exact *means* by which the call was intercepted. For example, plaintiffs would need to show where the call was intercepted and how the interception was accomplished in a physical sense. At least with respect to the allegation that NSA computers "scan" the contents of calls for particular names, numbers, words, or phrases, Am. Compl. ¶ 39, the precise mechanism by which such monitoring allegedly occurred would be vital to determining if it constituted the "acquisition" of call content in a legal sense. In addition, the court would need to determine precisely what, if anything, AT&T did in order to adjudicate whether plaintiffs can recover *from AT&T*. As the Fourth Circuit concluded, the state-secrets privilege bars discovery of "the roles, if any, the defendants played in the events" plaintiffs allege. *El-Masri*, 2007 WL 625130, at *9. Such matters directly implicate secret sources and methods of intelligence gathering.

For its part, AT&T could not be deprived of the right to present any evidence relevant to supporting its case. An obvious issue in this regard is whether the President had authority under Article II of the Constitution to acquire the content of calls without a warrant. *See* Brief for the United States at 38. The only

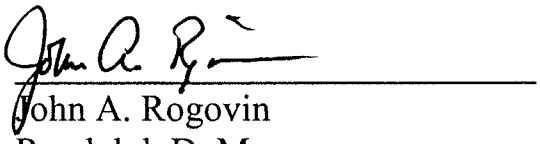
court to have addressed the issue concluded that FISA could not encroach on the President's constitutional authority to conduct warrantless surveillance. *In re Sealed Case*, 310 F.3d 717, 742 (Foreign Int. Surv. Ct. Rev. 2002). In any event, to impose liability in this case, it would be necessary to conclude that the general statutory strictures of FISA precluded the President's exercise of his constitutional powers in the specific circumstances of defending against the al Qaeda threat. To find that FISA trumps the President's power in this instance would require, at a minimum, inquiry into the magnitude and immediacy of the threat, the importance of the information in addressing the danger, and the inadequacy of alternative means of obtaining such information. These determinations, in which the President has said he was personally involved, are matters of the utmost secrecy and wholly unsuited for discovery or judicial examination. Because such evidence would be relevant to AT&T's defense, and because its secrecy prevents it from being adduced, the case cannot be fully and fairly litigated and hence must be dismissed.

CONCLUSION

The judgment of the District Court should be reversed and the case dismissed.

Respectfully submitted,

Dated: March 20, 2007



John A. Rogovin
Randolph D. Moss
Samir C. Jain
WILMER CUTLER PICKERING HALE AND DORR LLP
1875 Pennsylvania Avenue, NW
Washington, DC 20006
(202) 663-6000

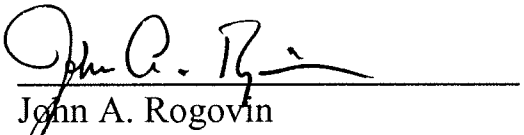
Henry Weissmann
MUNGER, TOLLES & OLSON LLP
355 South Grand Avenue, 35th Floor
Los Angeles, CA 90071-1560
(213) 683-9100

Attorneys for Amicus Curiae Verizon Communications Inc.

CERTIFICATE OF COMPLIANCE PURSUANT TO FED R. APP. P. 32(A)(7)(C) AND CIRCUIT RULE 32-1

I certify that pursuant to Federal Rule of Appellate Procedure 32(a)(7)(C) and Ninth Circuit Rule 32-1, the attached BRIEF OF *AMICUS CURIAE* VERIZON COMMUNICATIONS INC. IN SUPPORT OF APPELLANTS is proportionately spaced, has a typeface of 14 points or more, contains 6,262 words, and therefore complies with the 7,000-word limit authorized by Federal Rules of Appellate Procedure 29(d) and 32(a)(7)(B).

March 20, 2007



John A. Rogovin
Attorney for *Amicus Curiae*
Verizon Communications Inc.

CERTIFICATE OF SERVICE

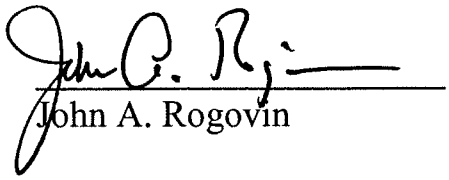
I hereby certify that on March 20, 2007, I caused copies of the foregoing BRIEF OF *AMICUS CURIAE* VERIZON COMMUNICATIONS INC. IN SUPPORT OF APPELLANTS to be served by overnight delivery on the following individuals:

Douglas N. Letter
Thomas M. Bondy
Anthony A. Yang
Attorneys, Appellate Staff
Civil Division, Room 7513
U.S. Department of Justice
950 Pennsylvania Ave., N.W.
Washington, D.C. 20530
(202) 514-3602
Counsel for the United States

Bradford A. Berenson
David Lawson
Edward McNicholas
Sidley Austin, LLP
1501 K Street, N.W.
Washington, D.C. 20005
(202) 736-8010
Counsel for AT&T

Robert D. Fram
Michael Markman
Heller Ehrman, LLP
333 Bush Street
San Francisco, CA 94104-2878
(415) 772-6000
Counsel for Plaintiffs-Appellees

I also certify that on this 20th day of March 2007, I filed the foregoing BRIEF OF *AMICUS CURIAE* VERIZON COMMUNICATIONS INC. IN SUPPORT OF APPELLANTS by sending the document via overnight courier for next-day delivery to the Clerk, United States Court of Appeals, 95 Seventh Street, San Francisco, California 94103-1526.



John A. Rogovin