PETER D. KEISLER
Assistant Attorney General, Civil Division
CARL J. NICHOLS
Deputy Assistant Attorney General
JOSEPH H. HUNT
Director, Federal Programs Branch
ANTHONY J. COPPOLINO
Special Litigation Counsel
tony.coppolino@usdoj.gov
ANDREW H. TANNENBAUM
Trial Attorney
andrew.tannenbaum@usdoj.gov
U.S. Department of Justice
Civil Division, Federal Programs Branch
20 Massachusetts Avenue, NW
Washington, D.C. 20001
Phone: (202) 514-4782/(202) 514-4263
Fax: (202) 616-8460/(202) 616-8202
*Attorneys for the United States of America*

**UNITED STATES DISTRICT COURT**

**NORTHERN DISTRICT OF CALIFORNIA**

**SAN FRANCISCO DIVISION**

| | |
|---|---|
| IN RE NATIONAL SECURITY AGENCY TELECOMMUNICATIONS RECORDS LITIGATION<br><br>This Document Relates To:<br><br>(1) All Actions Against the *MCI* and *Verizon* Defendants in the Master MCI and Verizon Consolidated Complaint, Dkt. 125; (2) *Bready v. Verizon Maryland* (06-06313); (3) *Chulsky v. Cellco Partnership d/b/a/ Verizon Wireless* (06-06570); (4) *Riordan v. Verizon Communications* (06-03574). | **No. M:06-cv-01791-VRW**<br><br>**REPLY MEMORANDUM OF THE UNITED STATES IN SUPPORT OF MILITARY AND STATE SECRETS PRIVILEGE AND MOTION TO DISMISS OR FOR SUMMARY JUDGMENT**<br><br>Hon. Vaughn R. Walker<br>Date: August 30, 2007<br>Time: 2:00 p.m.<br>Courtroom: 6 |

## (U) TABLE OF CONTENTS

# (U) TABLE OF AUTHORITIES

## Cases

**U.S. Constitution**



**Rules, Statutes, Legislative History**

## (U) INTRODUCTION

**(U)** In their opposition to the United States' motion to dismiss or for summary judgment ("Pl. Opp."), Plaintiffs admit that they challenge alleged foreign intelligence activities that are "far broader" and different than the publicly-acknowledged interception of the content of international communications to or from the United States reasonably believed to involve a member or agent of al Qaeda ("Terrorist Surveillance Program" or "TSP"). Pl. Opp at 3. Plaintiffs also concede that it is "uncontroversial" that "the disclosure of general facts about a [classified] program does not necessarily compel further disclosures of its operational details." *Id.* at 26. Yet, based precisely on such general facts about the limited TSP, Plaintiffs seek to compel the sweeping disclosure of National Security Agency ("NSA") operations that would be necessary to litigate their claims regarding alleged activities markedly different from what the United States has acknowledged—namely, an alleged dragnet of content surveillance involving the NSA's access to "all or a substantial number of the communications transmitted through [Verizon/MCI's] key domestic telecommunications facilities," Master Verizon Compl. ¶ 168, and an alleged telephone records program pursuant to which Verizon and MCI purportedly have been "providing tens of millions of call records to the NSA," Pl. Opp. at 2. In fact, as this Court has noted, the United States has *denied* the type of content dragnet alleged by Plaintiffs.

**(U)** Plaintiffs attempt to keep their claims alive by relying on various faulty and misguided arguments about the state secrets privilege and its impact on this case. The fundamental flaw in Plaintiffs' brief is that it openly invites the Court—based only on limited, ambiguous, and unreliable public statements—to discard the views of the Director of National Intelligence ("DNI") regarding the exceptional national security harms that could result from the disclosure of certain intelligence-related information. Such an approach is an invitation to error. Instead, as the cases make clear, the relevant inquiry is whether, after examining the classified and unclassified submissions of the DNI and NSA Director and affording those top intelligence officials the "utmost deference," the Government has demonstrated a "reasonable danger" that

disclosure of the information at issue will harm the national security. The predictive judgment of these top intelligence officials must be given the "utmost deference." Any other approach would improperly usurp the DNI's considered expertise regarding such matters.

**(U)** In addition to inviting the Court to apply an erroneous legal standard, Plaintiffs' presentation of the public statements regarding their call records allegations is inadequate and even misleading; as we demonstrate below, it contains material omissions and is based almost entirely on non-Executive Branch statements. Simply put, there has been no official confirmation or denial of an alleged call records program since this Court's decision in *Hepting v. AT&T*, 439 F. Supp. 2d 974 (N.D. Cal. 2006). And because the DNI and NSA Director have demonstrated that substantial harm to national security will result from litigating Plaintiffs' allegations regardless of the public statements, the Court should uphold the privilege assertion.

**(U)** Plaintiffs' brief also rests on the premise that it would be proper, at this stage of the litigation, for the Court to decide only whether the "very subject matter" of the case is a secret, and solely for the purpose of deciding whether their complaints can survive a motion to dismiss. Again, this argument rests on a faulty analysis of the state secrets doctrine; where, as here, a plaintiff challenges undisclosed and unconfirmed intelligence activities, and information subject to the state secrets privilege goes to the core of the plaintiff's claims, the "very subject matter" of the case is a state secret and the case must be dismissed.

**(U)** Even if there were doubt about concluding that the "very subject matter" of this case involves state secrets, the assertion of the state secrets privilege requires dismissal, at this time, for other reasons. For example, because evidence as to whether or not individuals are subject to intelligence activities cannot be disclosed without revealing the existence, scope, or nature of intelligence sources and methods, it is presently apparent that Plaintiffs cannot prove they have standing by being subject to any alleged NSA activities. It is no answer for Plaintiffs to argue that their *pleadings* are sufficient; the Government's summary judgment motion requires Plaintiffs to demonstrate *now* how they could prove their standing absent state secrets, and it is

plain that they cannot.

**(U)** It is also apparent now that Plaintiffs cannot make a *prima facie* case absent information subject to the state secrets privilege. For example, Plaintiffs cannot prove their claims without establishing that Verizon or MCI was involved in the challenged activities; but the DNI has demonstrated that the alleged relationships in this case cannot be confirmed or denied without harming national security. Plaintiffs similarly could not prove whether the alleged activities exist, the scope and duration of any such activities, whether Plaintiffs were personally subject to such activities, and whether the alleged activities operated in such a way that Plaintiffs' communications or records (even if within the potential scope of the activities) were actually "intercepted" or "disclosed"—all necessary elements of their case-in-chief. And as we have previously demonstrated, it is apparent now that Verizon and MCI could not defend this litigation itself absent state secrets. *See* Section IV, *infra*.

**(U)** Plaintiffs finally ask the Court to defer deciding many of the key state secrets questions so that they may first attempt to take discovery. But Plaintiffs' Rule 56(f) statement demonstrates why dismissal or summary judgment for the Defendants is appropriate at this stage. If this case were allowed to proceed, Plaintiffs indicate that they would seek discovery into, *inter alia*, facts needed to prove whether the alleged content dragnet and call records activities exist, whether Verizon and MCI were involved in such activities, and whether Plaintiffs' personal communications and records were intercepted or disclosed as part of such activities. *See* Section III, *infra*. But that information is squarely covered by the privilege, and Plaintiffs' 56(f) statement is an acknowledgment that such basic information remains secret from them. It is thus clear that delaying full resolution of the state secrets issues would be pointless and would defeat the very purpose of the privilege by putting the security of the information at continued risk of disclosure, inadvertent or otherwise.

**(U)** Dismissal at the outset is not unusual in a case like this; it is what the state secrets doctrine, as articulated by the Supreme Court and Ninth Circuit, requires. It is also the course

followed recently by the Sixth Circuit in *ACLU v. NSA*, in which the two judges in the majority held that the state secrets privilege prevented the plaintiffs from proving their standing, and in which all three judges agreed to uphold the dismissal of the plaintiffs' "datamining" claims, which were in all relevant respects the same as Plaintiffs' call records claims here. *See ACLU*, __ F.3d __, 2007 WL 1952370 (6th Cir. July 6, 2007).

**(U)** While Plaintiffs argue that this Court's decision in *Hepting* mandates the denial of our motion to dismiss or for summary judgment, we have explained our respectful disagreements with that decision and ask the Court to approach this case with a fresh perspective. Since *Hepting*, moreover, the TSP has been replaced with surveillance authorized by the Foreign Intelligence Surveillance Court, and there has been much congressional oversight of NSA activities. Given those developments, and the political processes at work to address these issues, the Court should avoid any unnecessary judicial determinations of the underlying constitutional and statutory questions presented by this case. It should also do everything within its power to avoid the disclosure of intelligence-related information that could harm the Nation for many years to come. We respectfully submit that, in this case, the only way to avoid such disclosures is through dismissal.

**[REDACTED TEXT]**

## (U) ARGUMENT

### I. (U) PLAINTIFFS INCORRECTLY APPLY THE STANDARD FOR REVIEWING AN ASSERTION OF THE STATE SECRETS PRIVILEGE

**(U)** The standard for determining whether to uphold an assertion of the state secrets privilege is well established: Affording the United States and its predictive judgments about the harm of disclosure the "utmost deference," a court must uphold the privilege assertion if it is satisfied that the government has demonstrated a "reasonable danger" that disclosure of the information will harm the national security. *United States v. Reynolds*, 345 U.S. 1, 10 (1953);

*Kasza v. Browner*, 133 F.3d 1159, 1166 (9th Cir. 1998); *Zuckerbraun v. General Dynamics Corp.*, 935 F.2d 544, 547 (2d Cir. 1991); *In re United States*, 872 F.2d 472, 475 (D.C. Cir. 1989); *Halkin v. Helms*, 598 F.2d 1, 9 (D.C. Cir. 1978) ("*Halkin I*" ) (quoting *United States v. Nixon*, 418 U.S. 683, 710 (1974)).

**(U)** Plaintiffs, however, urge the Court to apply a materially different two-part test to evaluate the state secrets privilege assertion in this case. First, Plaintiffs argue, the Court should put aside any conclusion by the Director of National Intelligence that an official confirmation, denial, or disclosure of the information at issue would harm the national security, and instead determine from other sources whether the information at issue is actually secret. *See* Pl. Opp. at 16. According to Plaintiffs, this secrecy determination should be made by looking at any information in the public record that may be deemed "reliable," including statements made by private individuals or entities and non-Executive Branch officials. *Id.* at 16-18. If such information exists in the public record in any form, Plaintiffs argue, it cannot be secret and the inquiry is at an end without giving *any* consideration to the DNI's conclusions regarding harm. *See id.* at 16-17. Only if there is a lack of such public information, would the Court determine whether the information's "verification or substantiation possesses the potential to endanger national security," *id.* at 16 (internal quotation marks omitted)—an inquiry in which Plaintiffs would give the DNI's conclusions only "some measure of deference," *id*.

**(U)** Plaintiffs' two-step approach lacks any foundation in law and is an invitation to error. *See* Memorandum of the United States in Support of the Military and State Secrets Privilege and Motion to Dismiss or for Summary Judgment ("U.S. Mem."), at 17-20 (submitted Apr. 20, 2007). By artificially separating the question of whether the information at issue is secret from whether disclosures would cause national security harm, and then looking to public allegations and information—but *not* the Director of National Intelligence's considered judgment—in

assessing secrecy, Plaintiffs would effectively render the DNI's judgment in this case irrelevant.[1] Such a result would turn the standard of review on its head.

**(U)** For both "constitutional" and "practical" reasons, the DNI's judgment must be the key consideration for the Court in reviewing the privilege assertion. *El-Masri v. United States*, 479 F.3d 296, 305 (4th Cir. 2007). As prior courts have correctly acknowledged, "the probability that a particular disclosure will have an adverse effect on national security is difficult to assess, particularly for a judge with little expertise in this area." *Ellsberg v. Mitchell*, 709 F.2d 51, 57 n.31 (D.C. Cir. 1983); *see also Halkin I*, 598 F.2d at 9 ("The courts, of course, are ill-equipped to become sufficiently steeped in foreign intelligence matters to serve effectively in the review of secrecy classifications in that area.") (quoting *United States v. Marchetti*, 466 F.2d 1309, 1318 (4th Cir. 1972)). Similarly, it is well understood that "the Executive and the intelligence agencies under his control occupy a position superior to that of the courts in evaluating the consequences of a release of sensitive information." *El-Masri*, 479 F.3d at 305. Indeed, "the executive branch's expertise in predicting the potential consequences of *intelligence disclosures* is particularly important given the sophisticated nature of modern intelligence analysis." *Id.* (emphasis added). It is for these fundamental reasons that courts have assessed state secrets assertions under a "narrow" standard of review that is centered around providing the "utmost deference" to the Executive. *Kasza*, 133 F.3d at 1166. Plaintiffs would completely gut this standard by removing the expert government official—the Nation's leading intelligence officer—from the dispositive step in their analysis.

**(U)** Among other defects, Plaintiffs' approach fails to recognize that confirming or denying information can harm the national security even if some information appears to exist already in the public domain. As this Court noted in *Hepting*, "simply because . . . statements

---

[1] **(U)** *See* Pl. Opp. at 16-17 (arguing that the Government's explanations of harm are "immaterial" if the information has been revealed "through reasonably reliable public statements").

have been publicly made does not mean that the truth of those statements is a matter of public knowledge and that verification of the statement is harmless." 439 F. Supp. 2d at 990; *accord Fitzgibbon v. CIA*, 911 F.2d 755, 766 (D.C. Cir. 1990) ("[W]e have unequivocally recognized that the fact that information resides in the public domain does not eliminate the possibility that further disclosures can cause harm to intelligence sources, methods and operations."). That is especially true in this Internet age where issues of public importance are likely to spawn legions of conflicting factual accounts and opinions, any one of which may be available at the touch of a button and all of which, together, inevitably create some measure of uncertainty. Even if an overwhelming majority of the public believed a specific fact about our intelligence gathering to be true, confirmation of that fact by the United States or through the exacting procedures of litigation would add a level of certainty not otherwise obtained. Whether providing such certainty would harm the national security in a particular case is a question that can be answered properly only by the appropriate government officials who have the full panoply of intelligence and threat information before them, as well as the constitutional responsibility and expertise to make that determination.

**(U)** Plaintiffs ask the Court to disregard those officials and to attempt its own non-expert prediction about the harm of disclosure based solely on reports of public statements.[2] To be

---

[2] **(U)** In *Hepting*, the Court applied a narrower "secrecy" analysis than Plaintiffs suggest, indicating that it would only consider "public admissions or denials by the government [and] telecommunication companies" as sufficiently reliable. 439 F. Supp. 2d at 990. Nonetheless, as discussed below, *see* Section II.B.3, *infra*, and in our opening brief, *see* U.S. Mem. at 17-20, 30-31, we respectfully submit that such reliance on carrier statements is erroneous and contrary to established precedent. As discussed, the "substantial indicia of reliability" test utilized in *Hepting* failed to give proper consideration and deference to the DNI's judgment that official disclosures in litigation would cause harm regardless of what the telecommunication carriers may have said. 439 F. Supp. 2d at 990. The *Hepting* decision also cited no other cases applying such a test, *see id.*, and while the district court in *Terkel* suggested in dicta that it "may" be appropriate, under some circumstances, to consider carrier statements as sufficiently "reliable" for purposes of a state secrets inquiry, it cited only *Hepting* for the proposition, *Terkel v. AT&T*, 441 F. Supp. 2d 899, 913 (N.D. Ill. 2006).

sure, we do not claim that the public record is, in all cases, irrelevant to a court's assessment of a state secrets privilege assertion. But any examination of publicly available information must be for the sole purpose of answering the only relevant question at issue—whether the United States has demonstrated a "reasonable danger" that official disclosures would harm the national security. And in answering that question, the Court must afford the "utmost deference" to the DNI's predictive judgments, including any judgments about why harm would result from confirming or denying certain facts even in the face of information that Plaintiffs believe is already in the public domain. Indeed, the Court can only reject the privilege assertion if, after considering all of the Government's classified and unclassified submissions, it concludes that the explanations of harm offered by the DNI and NSA Director are unreasonable or incoherent.[3] *See Doe v. Tenet*, 329 F.3d 1135, 1154 (9th Cir. 2003) ("utmost deference" standard could be satisfied with a "minimally coherent explanation" of the potential harm to national security), *rev'd on other grounds*, *Tenet v. Doe*, 544 U.S. 1 (2005). As set forth below, we believe it is not possible to reach such a conclusion in this case.

**(U)** One final note on the standard of review is appropriate. Plaintiffs' brief contains a good deal of rhetoric about the importance of the Judiciary in this case and the danger of abdicating to the will of the Executive. Plaintiffs warn, for example, that adopting the Government's view of the privilege "would reduce the Judiciary to a mere functionary of the

---

[3] **(U)** For example, in *Ellsberg v. Mitchell*, the D.C. Circuit largely upheld the government's state secrets assertion, but rejected it with respect to one piece of information: the names of the Attorneys General who had authorized the surveillance at issue. *See* 709 F.2d at 59-60. Public affidavits submitted by the government in the case acknowledged that the wiretaps were "authorized by the Attorney General," and none of the *in camera* submissions explained why the names of those officials had to be concealed. *Id.* The Court did not adopt Plaintiffs' proposed framework and simply order the names released because the identity of Attorneys General are public. Rather, the Court looked at the issue from the perspective of harm, concluding that the government had not adequately shown why harm would result from the disclosure. *See id.* at 60 ("We cannot see, and the government does not even purport to explain, how any further disruption of diplomatic relations or undesirable education of hostile intelligence analysts would result from naming the responsible officials.").

Executive." Pl. Opp. at 17. They emphasize that the state secrets privilege "does not confer upon the Executive branch unilateral authority to terminated unwanted litigation," *id.* at 14, and remind us that "it is up to *the Court*—not the Government—to decide whether the state secrets privilege applies in a particular case," *id.* at 15 (emphasis in original). *See also id.* at 15 ("[A] court must not merely unthinkingly ratify the executive's assertion of absolute privilege, lest it inappropriately abandon its important judicial role.") (quoting *In re United States*, 872 F.2d at 475; *id.* at 15 n.11 ("The Judiciary's exercise of independent review over assertions of the privilege plays a critical role in sustaining governmental checks and balances.").

**(U)** By no means do we urge the Court to abdicate its judicial responsibilities. We fully appreciate the Court's important role in assessing the privilege assertion under the standards established by the Supreme Court. *See El Masri*, 479 F.3d at 312 (holding that "the state secrets doctrine does not represent a surrender of judicial control over access to the courts"). It is out of respect for that role that we have submitted detailed classified presentations (in this case and others), setting forth for the Court the specific information that needs to be protected and the harms that could result from disclosure. We have made such detailed presentations, even though the law does not require them, so that the Court may see for itself the serious dangers of litigating this case. *See Reynolds*, 345 U.S. at 10 ("[W]e will not go so far as to say that the court may automatically require a complete disclosure to the judge before the claim of privilege will be accepted in any case.").[4] We ask only that the Court carefully consider all of the information that we have provided and defer appropriately to the judgments of the national security experts as to the risk of harms.

---

[4] **(U)** *See also Reynolds*, 345 U.S. at 10 ("It may be possible to satisfy the court, from all the circumstances of the case, that there is a reasonable danger that compulsion of the evidence will expose military matters which, in the interest of national security, should not be divulged. When this is the case, the occasion for the privilege is appropriate, and the court should not jeopardize the security which the privilege is meant to protect by insisting upon an examination of the evidence, even by the judge alone, in chambers.").

## II. (U) UNDER THE PROPER STANDARD, THE STATE SECRETS PRIVILEGE ASSERTION IN THIS CASE MUST BE UPHELD

**(U)** If the proper standard of review is applied, there should be no question that the state secrets privilege assertion in this case must be upheld as to all information it covers. The Director of National Intelligence and NSA Director have, in their unclassified and classified submissions, explained in detail the information that must be protected and the grave harms that confirmation, denial, or disclosure could cause to the national security. In light of these robust presentations, and the "utmost deference" that they must be afforded, we respectfully submit that the Court could not conclude that the Government's predictions of harm lack reasonable basis. In the absence of such an adverse finding, the privilege assertion must be sustained.

**(U)** Notably, Plaintiffs do not challenge the DNI and NSA Director's demonstration of harm. Instead, Plaintiffs' singular response to the validity of the privilege assertion is that public disclosures have either already revealed the information at issue or have opened the door to further inquiry. Plaintiffs significantly overstate and even misrepresent the meaning of public statements to make it seem as if the Government has confirmed intelligence activities and information that it has not. Moreover, virtually all of the public statements on which Plaintiffs rely were made by individuals outside of the Executive Branch, and thus by definition could not abrogate the state secrets privilege. Indeed, as already explained, the fact that information may exist in the public domain in some form does not alleviate the harm that could result from a confirmation or denial through litigation. In any event, even assuming *arguendo* that the public statements stand for what Plaintiffs claim and are true, such information would not be sufficient to actually allow the adjudication of Plaintiffs' claims, and any attempt to proceed would risk the grave harms identified by the DNI.

### A. (U) The DNI and NSA Director Have Clearly Demonstrated a Reasonable Danger that the Disclosures Necessary to Litigate this Case Will Harm the National Security

**(U)** The explanations of the national security harms risked by this litigation are specific and thorough, made from an unparalleled perspective at the top of our Nation's Intelligence

Community, grounded in unique expertise, and eminently reasonable. As both the DNI and NSA Director explain in unclassified terms, the disclosure of information covered by the privilege assertion[5] would cause exceptionally grave damage to the national security by, for example, "reveal[ing] to foreign adversaries whether or not the NSA utilizes particular intelligence sources and methods," Public McConnell Decl. ¶ 13 (thus "compromis[ing] actual sources and methods," *id.*, or disclosing information about "the NSA's capabilities or lack thereof," *id.* ¶ 17); "replac[ing] speculation with certainty for hostile foreign adversaries who are balancing the risk that a particular channel of communication may not be secure against the need to communicate efficiently," *id.* ¶ 13; "disclos[ing] either who is being targeted—thus compromising that collection—or who is not being targeted, thus revealing to adversaries that an individual is a secure source for communicating or, more broadly, the methods being used to conduct surveillance," *id.* ¶ 14; and "revealing substantive intelligence knowledge of the United States," *id.* ¶ 12. *Accord* Public Alexander Decl. ¶¶ 13-19.

**[REDACTED TEXT]**

**(U)** Accordingly, the DNI and NSA Director have clearly demonstrated a "reasonable danger" that adjudicating Plaintiffs' claims will cause national security harm.

### B. (U) Public Statements Neither Confirm Plaintiffs' Allegations Nor Negate the Harm that Would Result From Disclosures in this Case

**(U)** Focusing almost entirely on their allegations of a telephone records program, Plaintiffs quote portions of public statements which, it is claimed, confirm the existence of such a program and MCI's involvement. But in recounting those statements, Plaintiffs often omit key

---

[5] **(U)** In unclassified terms, the information covered by the privilege assertion includes information that may be needed to demonstrate that the TSP was a limited program and that the NSA does not otherwise engage in the content surveillance dragnet alleged by Plaintiffs, as well as information that may tend to confirm or deny whether the NSA collects large quantities of communication records as Plaintiffs allege; whether Verizon or MCI assisted the NSA with any intelligence activities alleged by Plaintiffs; and whether the individual Plaintiffs have been subject to any alleged intelligence activities. *See* Public McConnell Decl. ¶ 11.

language, ascribe clear meaning to obviously vague language, credit the uninformed with definitive knowledge, and at times even pair unconnected quotations to give the appearance that an individual said something that he did not—altogether making for a misleading presentation that does not demonstrate that either an alleged records program or the participation of any particular carrier has been confirmed.

**(U)** Indeed, contrary to Plaintiffs' claim that "new public disclosures" now render it "indisputable" that telecommunications companies have been "providing tens of millions of call records to the NSA," Pl. Opp. at 2., no such disclosures have occurred. As before, the Government has made a specific point *not* to confirm or deny the existence of the alleged telephone records program, and its public statements repeatedly reflect that caveat. For this reason, every court to rule on the issue—including all three judges of the Sixth Circuit—has declined to permit the disclosure of whether such a program exists. *See ACLU*, 2007 WL 1952370, at *68 (Gilman, J., dissenting); *Hepting*, 439 F. Supp. 2d at 997-98; *Terkel*, 441 F. Supp. 2d at 917; *ACLU v. NSA*, 438 F. Supp. 2d 754, 765 (E.D. Mich. 2006), *rev'd on other grounds*, 2007 WL 1952370 (6th Cir. July 6, 2007). The public statements relied on by Plaintiffs, virtually none of which are new, do not change that conclusion. Almost all of the statements come from outside the Executive Branch, and Plaintiffs fail to account for the harm that could result if facts were confirmed or denied during litigation—harm that easily meets the standard for upholding the privilege assertion regardless of how the statements are interpreted. *See, e.g., Fitzgibbon*, 911 F.2d at 766 ("[I]n the arena of intelligence and foreign relations there can be a critical difference between official and unofficial disclosures.").[6]

---

[6] **(U)** *See also Terkel*, 441 F. Supp. 2d at 915 ("A disclosure must be both official and public for the fact at issue to be considered a matter of public knowledge for FOIA purposes."); *Washington Post v. United States Dep't of Defense*, 766 F. Supp. 1, 10 (D.D.C. 1991) ("[I]f the information in the public domain was not officially disclosed, official confirmation or acknowledgment of that information may be harmful to national security," because "'unresolved doubt may still remain in the minds of the United States' potential and actual adversaries.'"

(continued...)

**(U)** With regard to their allegations of a content surveillance dragnet, Plaintiffs simply argue that the limited disclosures about the TSP's existence have "opened the door" to a broader inquiry into the NSA's operations. But Plaintiffs admittedly do not challenge the TSP, and the very general acknowledgments about that program cannot possibly require the disclosure of classified information that would be needed to address Plaintiffs' very different claims of a massive content dragnet.

**1. (U) The Executive Branch Has Not Confirmed a Telephone Records Program**

**(U)** Plaintiffs first argue, implausibly, that the President and Attorney General themselves have confirmed the existence of the alleged telephone records program. Ignoring the Executive Branch's repeated refusals to confirm or deny such a program, Plaintiffs focus on selective snipets from only two press conferences, neither of which comes close to confirming anything of the sort. In the first, the President responded to a vague question about whether the government is "trolling through the lives of innocent Americans," and whether "ordinary people [should] feel that their privacy is invaded by the NSA compiling a list of their telephone calls." Pl. Ex. N at 2. Plaintiffs extract one sentence of the President's response—"The program he's asking about is one that has been fully briefed to members of the United States Congress, in both political parties.," *id.*—and claim that the President must have been confirming a records program because the "colloquy did *not* address content interception," Pl. Opp. at 5 (emphasis in original). But in portions of the President's answer that Plaintiffs chose to omit, and that preceded the sentence at issue, the President did in fact address content interception. *See* Pl. Ex. N. at 2 ("I've also been clear about the fact that we do not listen to domestic phone calls without court approval . . . . But if al Qaeda is calling into the United States, we want to know, and we want to know why."). Regardless, it is inconceivable to conclude that by using the word "program" in

---

[6](...continued)
(quoting *Military Audit Project v. Casey*, 656 F.2d 724, 744 (D.C. Cir. 1981))).

response to a vague question, the President was confirming allegations that the Executive Branch had previously and subsequently refused to confirm or deny. Indeed, the point of the President's statement was to convey that Congress had been briefed on intelligence activities, not to confirm any particular program. Lest there be any doubt, within 30 minutes of the President's press conference, White House Press Secretary Tony Snow confirmed that the President "was not giving a back-handed confirmation" of the alleged records program—allegations "which we'll neither confirm or deny"—and that the President instead "was talking about foreign-to-domestic calls." Pl. Ex. R. at 1. Plaintiffs fail to mention Mr. Snow's statement.

**(U)** The second statement Plaintiffs rely on is an answer given by the Attorney General in response to a question about the telephone records allegations. In the very first sentence of his answer, which again Plaintiffs omit, the Attorney General states that "[t]here has been no confirmation about any details relating to the *USA Today* story." Pl. Ex. O at 7. That statement alone is sufficient to rebut Plaintiffs' claim that the Attorney General was confirming an alleged records program. But even if the Attorney General had not been that explicit, the portions of his answer actually quoted by Plaintiffs simply reflect that the *USA Today* story concerned allegations about business records and that, as a general matter, there are "a number of legal ways, of course, that the government can have access to business records," including by "issu[ing] national security letters" through "the FBI." *Id.* This was clearly a general statement about available legal mechanisms to collect business records, not a confirmation of any alleged intelligence program.

**(U)** Later in their brief, Plaintiffs make the misleading assertion that "[b]oth President Bush and Attorney General Gonzales have acknowledged the existence of a program 'that has been fully briefed to members of the United States Congress' and entails 'the NSA compiling a list of [Americans'] telephone calls.'" Pl. Opp. at 24. It is misleading because the second quotation in the sentence is a quote not from the President or Attorney General, but from a member of the press. It is also wrong, for the reasons described above.

**(U)** Plaintiffs point to no other public Executive Branch statements that, in their view, confirm or deny the alleged telephone records program, nor could they. As reflected in the several court decisions on point, for over a year now the United States has repeatedly refused to confirm or deny such allegations. *See, e.g.*, *Terkel*, 441 F. Supp. 2d at 914 (holding that there were no Executive Branch disclosures concerning the telephone records allegations). Indeed, as recently as this week the DNI publicly reiterated that the TSP is the only NSA program that has been officially acknowledged (and that the operational details of the TSP "have not been made public and cannot be disclosed without harming national security"). *See* Letter from Director of National Intelligence, J.M. McConnell to Senator Arlen Specter (July 31, 2007) (attached as Exhibit A).

**2. (U) Congress Has Not Confirmed a Telephone Records Program**

**(U)** Plaintiffs next argue that members of Congress have confirmed the existence of a telephone records program. But a closer examination of those statements, and the portions that Plaintiffs omit, demonstrate otherwise. For example, Plaintiffs cite an answer that Senator Pat Roberts gave to a question about the *USA Today* story, in which he stated very generally that "if you want to get into that, we're talking about business records." Pl. Ex. P at 2. That comment is no different, however, from the Attorney General pointing out that the *USA Today* story concerned allegations about business records, in order to distinguish the legal landscapes governing content collection and records collection. And Senator Roberts was very careful to state, a number of times, that he "can't comment on the accuracy [of] the articles in the *New York Times* or the *USA Today*," or "get into the specifics of" classified activities—caveats which Plaintiffs do not mention. *Id.* at 2, 3.[7]

[7] **(U)** Plaintiffs also refer to a CBS news report which does not quote Senator Roberts, but instead states, without any direct quotations, that Senator Roberts told a CBS correspondent that the NSA was looking at the pattern of phone calls collected during the surveillance. *See* Pl. Opp. at 6. This double hearsay and apparent paraphrasing clearly does not meet even the (continued...)

**(U)** Plaintiffs also cite an interview given by Senator Kit Bond, but even Plaintiffs acknowledge that Senator Bond specifically stated that he was "not commenting on in any way any of the allegations made in the [*USA Today*] story today." Pl. Ex. T at 5; Pl. Opp. at 7. Senator Bond's general statement that "business records are not protected by the Fourth Amendment," *id.* at 4, is, again, a generic legal point that makes complete sense to offer in light of the *allegations* in the *USA Today* story (indeed, the United States has made the same point in this litigation in light of Plaintiffs' allegations, *see* U.S. Mem. at 53). Similarly, in another interview cited by Plaintiffs, Senator Bill Frist states that he is "not going to comment" on the alleged telephone records program and that "[t]here has not been even a confirmation" of the *USA Today* story. Pl. Ex. U at 18. Plaintiffs, once again, omit those portions from their brief.[8]

**(U)** Finally, Plaintiffs cite an additional *USA Today* article which reported that unnamed lawmakers confirmed that the NSA compiled a database of telephone records. *See* Pl. Ex. W; Pl. Opp. at 8. Such hearsay involving unnamed sources is clearly unreliable; indeed, the Court has already rejected reliance on news articles in general.[9] *See Hepting*, 439 F. Supp. 2d at 991

---

[7](...continued)
reliability standard proffered by Plaintiffs. *See Hepting*, 439 F. Supp. 2d at 991. And it says nothing about the collection of large quantities of phone records. Rather, it suggests that the calls collected during the targeted content surveillance were also examined for patterns. The same story, moreover, also reiterates the government's refusal to confirm or deny the telephone records allegations. *See* Pl. Ex. Q at 1 ("Mr. Bush declined to specifically discuss the compiling of phone records . . . ."); *id.* at 2 ("'You're assuming that the program exists, and we neither confirm nor deny it,' [Tony] Snow said.").

[8] **(U)** Plaintiffs also cite a statement by Representative Jane Harman, in a hearing concerning the Department of Homeland Security, that "there is a program that involves the collection of *some* phone records." Pl. Ex. X at 8 (emphasis added). This statement, however, is so general and vague that it is not even clear which agency runs the program Representative Harman is referring to (the NSA is not the subject of the hearing, nor is it mentioned), or what the scope of any collection may be.

[9] **(U)** Although the article does contain some quotes from named congressional sources, those quotes are vague, sometimes conflicting, and divorced from any context that would make it (continued...)

(declining to "rely on media reports about the alleged NSA programs because their reliability is unclear"); *Terkel*, 441 F. Supp. 2d at 914 (rejecting reliance on the same *USA Today* article); *see also El-Masri*, 479 F.3d at 311 n.5 (declining to endorse plaintiff's theory that information is ineligible for protection under the state secrets privilege simply because it has been published in the news media); *Edmonds v. FBI*, 272 F. Supp. 2d 35, 49 (D.D.C. 2003) (where "statements in the press were made by anonymous sources, even documents containing identical information may properly be withheld [under FOIA] because release would amount to official confirmation or acknowledgment of their accuracy") (internal quotation marks omitted).[10] In addition, the article reiterates that the President, Attorney General, and National Security Advisor all stated that they could not confirm or deny the telephone records allegations, thereby making clear even to those who believe the story that there is a considerable lack of certainty regarding the allegations. Pl. Ex. W at 3.

**(U)** The public record thus demonstrates that no member of Congress has confirmed or denied an alleged telephone records program. Indeed, any suggestion that members of Congress intended their statements to be used to compel the disclosure of alleged intelligence sources and methods should not be credited. The most that can be said is that these lawmakers have tried to address allegations about intelligence activities—a matter of public concern—without seeking to reveal classified information. In any event, statements by individual members of Congress cannot abrogate a state secrets assertion. It is well established that the "authority to protect

---

[9](...continued)
clear what specifically was being discussed. For example, Senator Orrin Hatch is quoted as saying only "[i]t was within the president's inherent powers," Pl. Ex. W at 3, but it is far from clear what he meant by "it." (He could have been referring, for example, to the TSP.)

[10] **(U)** For the same reasons, the Court should not rely on a recent *New York Times* article that cites unnamed and anonymous sources in reporting that "[a] 2004 dispute over the National Security Agency's secret surveillance program . . . involved computer searches through massive electronic databases." Scott Shane & David Johnston, *Mining of Data Prompted Fight Over Spying*, N.Y. Times, July 29, 2007, at A1.

[national security] information falls on the President as head of the Executive Branch and as Commander in Chief," *Department of the Navy v. Egan*, 484 U.S. 518, 527 (1988), and that the state secrets privilege likewise is grounded in Article II of the Constitution, *see United States v. Nixon*, 418 U.S. at 710-11. Because the Executive Branch is constitutionally charged with the control of such information (and, unlike other branches or entities, has the complete view of such information), only disclosures by the Executive can be expected to be official and fully accurate. *See, e.g., Salisbury v. United States*, 690 F.2d 966, 971 (D.C. Cir. 1982) ("[B]are discussions by this court and the Congress of NSA's methods generally cannot be equated with disclosure by the agency itself of its methods of information gathering.");[11] *Edmonds v. United States Dep't of Justice*, 323 F. Supp. 2d 65, 76 (D.D.C. 2004) ("That privileged information has already been released to the press or provided in briefings to Congress does not alter the Court's conclusion" that "the invocation of the state secrets privilege is proper."); *see also Edmonds v. FBI*, 272 F. Supp. 2d at 49 ("disclosure of information to a congressional committee does not constitute a waiver" of the Executive's "right to classify the information" or to withhold it under FOIA).

**(U)** That is particularly evident in this case, where the hodgepodge of individual congressional statements cited by Plaintiffs are often vague, confusing, and without context.[12] As one such statement expressly acknowledges, there is much "misinformation" in the public

---

[11] **(U)** Plaintiffs argue that *Salisbury* stands only for the "uncontroversial proposition that the disclosure of general facts about a program does not necessarily compel further disclosures of its operational details." Pl. Opp. at 26. While we agree that such a proposition is uncontroversial, the statement at issue in *Salisbury* does not make the "general facts" versus "operational details" distinction; rather, it simply says that the disclosure by Congress of "NSA's methods" cannot be equated with disclosure by the agency itself "of its methods." *Salisbury*, 690 F.2d at 971.

[12] **(U)** Indeed, the forums in which many of the statements cited by Plaintiffs were made (such as live television interviews) are inherently susceptible to producing vague, incomplete, or inaccurate information. Questions and answers may be misheard or misunderstood, participants may not have enough time to articulate their thoughts with clarity or nuance, responses may be made assuming an unexpressed context, and a phrase or comment may easily be misconstrued to suggest a meaning not intended.

domain. Pl. Ex. P at 2. Confusion and uncertainty thus persist regardless of what individual members of Congress have said in response to the *USA Today* story.[13] In such an atmosphere, any confirmation or denial of the telephone records allegations through this litigation would undoubtedly harm the national security by providing foreign adversaries with a certainty about U.S. intelligence operations that is currently absent.

**(U)** The district court in *Terkel* recognized additional reasons not to look statements by individual members of Congress in assessing the state secrets privilege assertion:

> Treating confidential statements to Congressional representatives as public disclosures that make an otherwise secret activity a matter of public knowledge would undermine the state secrets privilege by forcing the executive branch to give up the privilege whenever it discusses classified activities with members of Congress. Just as importantly, it would also discourage executive officials from candidly discussing intelligence activities with Congress, further reducing the legislative branch's ability to hold executive officials accountable.

441 F. Supp. 2d at 914. For these reasons and those discussed above, the statements cited by Plaintiffs do not undercut the DNI's state secrets assertion, nor do they alleviate the significant harm that could occur from the disclosures that would be necessitated by this case.

**[REDACTED TEXT]**

### 3. (U) Verizon/MCI Has Not Confirmed a Telephone Records Program

**(U)** Citing a "pre-recorded statement" by a Verizon Wireless Regional President and

---

[13] **(U)** The fact that Congress has not spoken with a collective and considered voice further undercuts any argument that an official disclosure occurred and sharply distinguishes this case from *Jabara v. Kelley*, 75 F.R.D. 475 (E.D. Mich. 1977), which involved the publication of a fact in a congressional committee report, *see id.* at 493. Although the Court need not answer in this case whether a disclosure in a congressional report would abrogate a particular state secrets assertion, it is significant to note that the D.C. Circuit has held that the government was "doubtless correct" in arguing that "executive branch confirmation or denial of information *contained in congressional reports* could under some circumstances pose a danger to intelligence sources and methods." *Fitzgibbon*, 911 F.2d at 766 (emphasis added); *see also Terkel*, 441 F. Supp. 2d at 914 (disagreeing with *Jabara*).

anecdotes about conversations with Verizon customer service representatives, Plaintiffs attempt to argue that Verizon itself has confirmed the existence of a telephone records program. Pl. Opp. at 9 & n.8. That attempt falls flat. First, of course, Verizon Wireless is not a defendant in this action, and there is no reason to impute the statement to the existing Verizon/MCI Defendants.[14] Second, there is no basis in the record to conclude that a Regional President of Verizon Wireless would have any knowledge about alleged classified intelligence activities, let alone activities allegedly concerning other Verizon/MCI entities at which the Regional President was not employed. Third, the statement on which Plaintiffs rely—"We were asked, but we said, no, we would not give that information, again, you know, trying to protect the privacy of our customers," Pl. Ex. Z at 3—is devoid of any specifics or context. It is completely unclear, for example, what "information" is at issue, who "asked" for that information, or who was asked. And because the statement is simply an excerpt presented as part of an edited series of clips, it is not even evident what question the statement intended to answer. *Id.* Fourth, there is no basis to believe that the many customer service representatives employed by Verizon worldwide would possess classified information about alleged intelligence activities, and any suggestion to the contrary is simply not credible. Accordingly, Plaintiffs' claim of a Verizon disclosure is easily rebutted.

**(U)** The same is true of Plaintiffs' claim that Verizon press statements reveal that MCI participated in a telephone records program. As Plaintiffs concede, the company's press releases do *not* state that MCI provided customer telephone records to the NSA. *See* Pl. Opp. at 9. Instead, Plaintiffs argue that the statements could be interpreted as an implicit acknowledgment that MCI provided such records. *See id.* at 9-10. While Plaintiffs are entitled to their own interpretation of the press releases, that type of speculation certainly cannot be equated with an official disclosure. *See Terkel*, 441 F. Supp. 2d at 912 n.6 (noting that it was "unclear" from the

[14] **(U)** Plaintiffs voluntarily dismissed Verizon Wireless entities on March 30, 2007. *See* MDL Docket Nos. 223, 230.

press release as to whether MCI provided telephone records to the NSA prior to its acquisition by Verizon).

**(U)** Likewise, Verizon's statements do not alleviate the harm that would result from fully adjudicating Plaintiffs' claims on the subject. As Plaintiffs themselves demonstrate, many appear to believe that Verizon's press statements are open to interpretation or question. After all, Plaintiffs do not accept what Verizon said, as they continue to allege that Verizon has provided the NSA with call records "of all or substantially all of [its] customers" since October 2001. Master Verizon Compl. ¶ 169; *see also* Pl. Opp. at 9-10 n.8 (alleging that "Verizon customer service representatives have told customers that Verizon turned over call records of Verizon wireline customers to the NSA"). And a quick scan of just a few well-trafficked Internet blogs reveals a number of different views of the press releases and, in particular, whether Verizon may have assisted the NSA.[15] *See also Hepting*, 439 F. Supp. 2d at 991 (noting that public statements by Verizon and BellSouth conflicted with an earlier *USA Today* article). Given the continuing uncertainty surrounding the carrier statements, any confirmation or denial of Plaintiffs' allegations through litigation would clearly clarify the conflicting public perceptions and thereby harm the national security.[16]

---

[15] **(U)** *See, e.g.*, Talking Points Memo, http://www.talkingpointsmemo.com/archives/008482.php (May 16, 2006, 11:36 PM) ("For all the shilly-shallying, Verizon does appear to come right out and deny they gave any customer records to the NSA. So what gives? I think I've got the answer: they're lying."); Washington Monthly, http://www.washingtonmonthly.com/archives/individual/2006_05/008851.php (May 19, 2006, 6:52 PM) ("[Other bloggers] explore the possibility that the NSA actually worked with third-party billing and equipment vendors, not with the telcos themselves . . . This doesn't quite seem to add up to me, but you never know. It's a possibility."); Washington Monthly, http://www.washingtonmonthly.com/archives/individual/2006_05/008827.php (May 16, 2006, 8:54 PM) ("The telco denials are pretty flat, and if they're lying they're doing it clumsily. Why not just stick with 'no comment on national security matters' if the reports are true?").

[16] **(U)** The fact that Verizon and MCI may have provided some customer telephone records to the *FBI* in response to *individualized* requests made pursuant to National Security

(continued...)

**(U)** In any case, statements by private parties such as telecommunication carriers cannot constitute confirmations, denials, or disclosures for purposes of the state secrets privilege. As discussed in our opening brief, *see* U.S. Mem. at 30-31, the Supreme Court held in both *Totten v. United States*, 92 U.S. 105 (1875) and *Tenet v. Doe*, *supra*, that litigation over an alleged espionage relationship was barred, even though the plaintiffs in those cases were the alleged spies and obviously would have known if they had performed espionage services for the government. Likewise, the Fourth Circuit recently upheld the state secrets assertion in *El-Masri*, despite the fact that the plaintiff would have been a witness to his own alleged detention and maltreatment. *See* 479 F.3d at 308-09; *see also El-Masri v. Tenet*, 437 F. Supp. 2d 530, 538 (E.D. Va. 2006) ("It is self-evident that a private party's allegations purporting to reveal the conduct of the United States' intelligence services overseas are entirely different from the official admission or denial of those allegations."). Other courts have reached similar conclusions in cases where private parties had personal knowledge of the information at issue. *See, e.g., Black v. United States*, 62 F.3d 1115, 1117-19 (8th Cir. 1995) (upholding a state secrets assertion over information concerning the plaintiff's alleged contacts with CIA agents, even though the plaintiff would have known of his own contacts); *Fitzgerald v. Penthouse Int'l, Ltd.*, 776 F.2d 1236, 1237, 1242 & n.8 (4th Cir. 1985) (upholding state secrets privilege over information about a Department of Navy marine mammal program despite the fact that the plaintiff was involved with the program and had "*personal knowledge of classified matters within the scope of the*" privilege assertion) (emphasis added). These cases all recognize that the

---

[16](...continued)
Letters, *see* Pl. Opp. at 11-13, by no means confirms or suggests that the carriers have given the *NSA* access to *all* of their customers' records. It is no secret, of course, that statutory mechanisms allow or require the carriers to provide the government with telephone records of individual customers under certain circumstances. *See, e.g.*, 18 U.S.C. §§ 2702-03 (setting forth such circumstances). What is secret is whether the NSA utilizes a particular intelligence-gathering method that involves the collection and analysis of mass quantities of phone records, as Plaintiffs allege.

focal point of the analysis is whether a disclosure through litigation would cause harm, not whether private individuals or entities (even those presumed to have actual knowledge) have previously made, or could make, public statements or allegations.

**(U)** In sum, whether or not the Court chooses to take private party or congressional statements into account, such statements simply have not disclosed whether the alleged telephone records program exists, and surely have not provided our foreign adversaries with any measure of certainty. Thus, the public record in this case by no means undercuts the expert conclusions of the DNI and NSA Director that substantive harm will result from the confirmation, denial, or disclosure of the information at issue.

**4. (U) The Government's Minimal Disclosures Concerning Content Collection Neither Confirm Verizon/MCI's Alleged Participation in the TSP Nor Open the Door for a Fishing Expedition into NSA Activities**

**(U)** After focusing almost exclusively on their call records allegations, Plaintiffs briefly turn to the subject of content collection and argue that (1) the participation of Verizon and MCI in the TSP is not secret, and (2) the Government's acknowledgment of the TSP's existence allows Plaintiffs to test their dragnet allegations by probing into other NSA activities. Both of these contentions are meritless.

**(U)** Plaintiffs offer very little to support their first argument. Instead, they simply make the following highly misleading assertion in their brief: "Attorney General Gonzales has already disclosed the general contours and existence of the NSA program involving 'intercepts of contents of communications,' Ex. B at 1, whereby 'the N.S.A. has gained the cooperation of American telecommunications companies to obtain backdoor access to streams of domestic and international communications.' Ex. I at 1." Pl. Opp. at 27. The latter part of this quote is a description by a *New York Times* reporter, *not* the Attorney General, and thus Plaintiffs once again pair two unrelated quotes to make it appear as if the Government has confirmed something it has not. Indeed, as the actual quotes demonstrate, allegations that Verizon or MCI assisted with the TSP have not been confirmed or denied. *See* Section II.B.1, *supra*; *see also Hepting*,

439 F. Supp. 2d at 988 (noting that Verizon "declin[ed] to confirm or deny whether it had any relationship to the NSA program acknowledged by the President").

**(U)** Aside from Government statements (which provide Plaintiffs no support), Plaintiffs rely merely on the carriers' "ubiquity" and Verizon's general and unsurprising statement that it "always stands ready . . . to help protect the country from terrorist attack." Pl. Opp. at 28; Pl. Ex. BB. As we have already explained, there is no basis in the public record to conclude, simply because of the carriers' size, that the Government needed, requested, or received the assistance of Verizon or MCI in implementing the TSP. *See* U.S. Mem. at 32-33. And a general willingness to assist the Government does not mean that assistance was actually requested or given with respect to a particular intelligence program. The Verizon statement cited by Plaintiffs simply says that "*[w]hen* asked for help, [Verizon] will always make sure that *any* assistance is authorized by law and that [its] customers' privacy is safeguarded," Pl. Ex. BB (emphasis added); thus, contrary to Plaintiffs' suggestion, Verizon has not even said that it will always help when lawful. That is hardly a basis to argue that Verizon or MCI's alleged participation in the TSP has been confirmed.

**(U)** Plaintiffs' second argument—that official disclosures about the existence of the TSP "open the door" to the adjudication of their dragnet allegations—is likewise erroneous. Only the most general facts about the TSP have been disclosed, such as its existence and the fact that it targeted international communications involving members or agents of al Qaeda or affiliated terrorist organizations. Plaintiffs themselves concede it is "uncontroversial" that "the disclosure of general facts about a program does not necessarily compel further disclosures of its operational details," Pl. Opp. at 26, and that principle is certainly applicable here. Numerous other facts about the TSP and the NSA's operations remain highly classified, and forcing their disclosure based on the extremely limited public description of the TSP would, as the DNI explains, cause irreparable harm to the national security by compromising sensitive intelligence sources and methods.

**(U)** The few official disclosures about the TSP, in any event, are irrelevant to this case because Plaintiffs admittedly challenge a much different and "far broader" alleged activity. Pl. Opp. at 3. Instead of the "limited interceptions of international calls tha[t] [sic] the Government has disclosed," *id.*, Plaintiffs challenge a purported "widespread program of intercepting and monitoring domestic communications, *id.* at 23. *See also* Master Verizon Compl. ¶¶ 165, 167 (alleging that "the NSA intercepts millions of communications made or received by people inside the United States" as part of a "massive surveillance operation"); *id.* ¶ 168 (alleging that the NSA has "direct access to *all* or a substantial number of the communications transmitted through [Verizon/MCI's] key domestic telecommunications facilities, including direct access to streams of domestic, international, and foreign telephone and electronic communications") (emphasis added). Because adjudicating Plaintiffs' dragnet claim would require probing NSA activities beyond what has been publicly described, *see* U.S. Mem. at 3, 50, Plaintiffs effectively argue that the acknowledged existence of one limited intelligence activity allows them, simply by asserting speculative allegations, to force the disclosure of additional intelligence information or activities. The law does not allow such a "fishing expedition." *Sterling v. Tenet*, 416 F.3d 338, 344 (4th Cir. 2005). Certainly, if Plaintiffs concede that "the disclosure of general facts about a program does not necessarily compel further disclosures of its operational details," Pl. Opp. at 26, then they must also concede that the disclosure of general facts about one activity cannot compel further disclosures about *other* alleged activities.

**(U)** With respect, Plaintiffs' "opened-the-door" theory is far too simplistic and fails to take account of the fundamental principle underlying the state secrets privilege: where the United States has shown a "reasonable danger" that disclosure will harm the national security, the privilege must be upheld. *Reynolds*, 345 U.S. at 10. The DNI and NSA Director have amply demonstrated the harms that would occur if this litigation required the disclosure of classified intelligence information required to disprove Plaintiffs' dragnet theory. Ignoring their judgment and allowing Plaintiffs to probe the NSA for proof of any undisclosed operations would

essentially put the Nation's most sensitive foreign intelligence operations at risk any time a narrow public disclosure is made or a litigant chooses to speculate. *See Hepting*, 439 F. Supp. 2d at 990 (declining to "invite attempts to undermine the privilege by mere assertions of knowledge by an interested party").

* * *

**(U)** For all of these reasons, the Court should, after considering all of the information covered by the state secrets assertion and applying the utmost deference to the DNI and NSA Director's predictions of harm, find that the United States has demonstrated a reasonable danger that disclosure, confirmation, or denial of the covered information would harm the national security, and, accordingly, uphold the privilege assertion.

## III. (U) THE COURT MUST DECIDE THE FULL IMPACT OF THE STATE SECRETS PRIVILEGE ON THE PARTIES' ABILITY TO LITIGATE THIS CASE

**(U)** Once the state secrets privilege is upheld, the Court must determine the effect of the privilege on the case. In all cases the privilege requires the exclusion of the protected information from disclosure; in certain cases where state secrets are necessary to a full and fair adjudication of the case, the case cannot proceed and must be dismissed. *See, e.g.*, *El-Masri*, 479 F.3d at 306-08; *Kasza*, 133 F.3d at 1166. The Court should not defer dismissing the case when it is evident that the litigation will require state secrets; rather, in order to avoid proceedings that will unnecessarily risk the disclosure of state secrets, the Court must assess the full impact of the privilege at the time of the assertion.

**(U)** With respect, we believe that one of the key procedural errors in *Hepting* was the failure to fully assess the consequences of the privilege. *See* U.S. Mem. at 20-24. Plaintiffs in this case seek to compound that error by advocating for an artificial and false division between the "very subject matter" prong of the state secrets analysis and the *prima facie* case/defense prongs. For some reason, Plaintiffs believe that the "very subject matter" inquiry is the only appropriate state secrets question at this stage of the case and that all other questions concerning

the effect of the state secrets privilege must be put off until after discovery. *See* Pl. Opp. at 31-34. Plaintiffs thus argue that the United States' summary judgment motion is "premature," and that the state secrets issues presented by the motion should be considered only "as the individual evidentiary issues arise" and only after it is apparent whether a decision on the "very subject matter" issue will "fundamentally alter the landscape of this litigation." Pl. Opp. at 31, 34.

**(U)** While the "very subject matter" question is certainly a key issue, there is no basis for limiting the Court's review to that single question and delaying a decision on the *prima facie* case and defense prongs of the privilege. Indeed, the three prongs of the state secrets analysis are very much related and often overlap. For instance, there are cases (like this one) which should be dismissed—regardless of what non-privileged evidence the plaintiff may be able to produce to make out a *prima facie* case—simply because it is "so obvious" that the very subject matter inherently involves state secrets and "that the action should never prevail over the privilege." *Tenet*, 544 U.S. at 9 (emphasis in original) (quoting *Reynolds*, 345 U.S. at 11 n. 26); *see Kasza*, 133 F.3d at 1166; *Bareford v. General Dynamics Corp.*, 973 F.2d 1138, 1141 (5th Cir. 1992). But the "very subject matter" question is also intertwined with the evidentiary issues, because often the parties' inability to prove or defend the case without privileged information is the *reason* that the very subject matter of the case is secret. *See Fitzgerald*, 776 F.2d at 1243 ("Due to the nature of the question presented in this action *and* the proof required by the parties to establish or refute the claim, the very subject of this litigation is itself a state secret.") (emphasis added). As the Fourth Circuit recently recognized, both "the 'central facts' and 'very subject matter' of an action are those facts that are essential to prosecuting the action or defending against it." *El-Masri*, 479 F.3d at 308; *see also id.* at 311 (equating the "very subject matter" of an action with "the facts central to its litigation").

**(U)** In this case, the inquiries are so interrelated that they cannot be separated. Whether viewed as a "very subject matter" issue or a *prima facie* case/defense issue, the bottom line is that "the privileged information will be so central to the litigation that any attempt to proceed

will threaten that information's disclosure." *Id.* at 308. The Court can reach that conclusion either in connection with the motions to dismiss or in ruling on our motion for summary judgment.[17] But in either case, the necessary result is the same and the labels are ultimately immaterial.[18]

**(U)** Plaintiffs, moreover, are plainly wrong in arguing that "the Government has failed to cite a single factually analogous case supporting its insistence that this case be dismissed at the pleading stage." Pl. Opp. at 23; *see also id.* at 21 ("In truth, not *one* of the cases cited by the

---

[17] **(U)** *See, e.g.*, *El-Masri*, 479 F.3d at 311 (affirming grant of motion to dismiss "at the pleading stage" because state secrets were "facts central" to the litigation); *Kasza*, 133 F.3d at 1166 (if the privilege deprives the defendant of the ability to assert a valid defense, "then the court may grant summary judgment to the defendant"); *Zuckerbraun*, 935 F.2d at 547 ("Where the effect of the invocation of the privilege is to prevent the plaintiff from establishing a prima facie case, the dismissal is probably most appropriate under Rule 56 on the ground that the plaintiff, who bears the burden of proof, lacks sufficient evidence to carry that burden.").

[18] **(U)** The D.C. Circuit's decision in *In re Sealed Case*, No. 04-5313, 2007 WL 2067029 (D.C. Cir. July 20, 2007), does not compel a different result. That case concerned whether the plaintiff, an official at a U.S. embassy, could prove that his phone conversation had been intercepted by another embassy official in connection with a professional dispute. The district court granted the Government's motion to dismiss under Fed. R. Civ. P. 12(b)(6) on the grounds that state secrets precluded the plaintiff from making a *prima facie* case about the matter, deprived the defendants of information required in their defense, and went to the very subject matter of the case. The Court of Appeals agreed that the state secrets privilege did protect certain information, but found that the plaintiff could make a *prima facie* case *without* state secrets because he was in possession of a cable written by the defendant that quoted his phone conversation verbatim, and had sworn testimony from a party to the call allegedly intercepted that he had not disclosed the substance of the conversation. Assuming, *arguendo*, the Court was correct that this was sufficient for the plaintiff's *prima facie* case notwithstanding any underlying state secrets (an issue that the Government contests in that case), Plaintiffs here have no such evidence as to whether they personally were intercepted and could not make a *prima facie* case otherwise. Moreover, the Court in *In re Sealed Case* left open on remand whether state secrets ultimately would require dismissal. Here, in contrast, it should be apparent now that state secrets are essential to adjudicating every issue in this case. Finally, the Court's ruling on one aspect of the state secrets doctrine —that dismissal would be required only where a defense would be "dispositive"—is not well-founded as a matter of law and would lead to a number of serious concerns. *See id.* at * 13-19 (Brown, J. dissenting). In any event, Plaintiffs' claims here could not survive for the numerous reasons presented by the Government.

Government actually supports its position.") (emphasis in original). To the contrary, two cases exactly on point—*ACLU* and *Terkel*—have resulted in dismissal at the same stage, without discovery. Such a result, in fact, is not as rare as Plaintiffs claim; in the relatively small universe of state secrets cases, a number of actions have been dismissed at the outset for the precisely the reasons we have articulated. *See, e.g., El-Masri*, 479 F.3d at 311; *Sterling*, 416 F.3d at 347-48; *Zuckerbraun*, 935 F.2d at 547-48; *Edmonds*, 323 F. Supp. 2d at 78-79.[19] Plaintiffs cite no case supporting the notion that a court should allow a case to proceed even though it is apparent that privileged information is at the heart of the case and that further proceedings will be futile. *See Sterling*, 416 F.3d at 344 ("Once the judge is satisfied that there is a 'reasonable danger' of state secrets being exposed, any further disclosure is the sort of 'fishing expedition' the Court has declined to countenance.") (citation omitted).

**(U)** Plaintiffs' discovery requests vividly illustrate the futility of delaying a full assessment of the privilege in this case. Should the Court allow this case to proceed, Plaintiffs indicate that they would seek the following: (1) "[R]equests for admissions regarding *the facts of* MCI and Verizon's interception of Plaintiffs' communications for the Government," (2)

---

[19] **(U)** Plaintiffs' attempt to distinguish these cases fails. *See* Pl. Opp. at 21-22. Indeed, the cases illustrate well the Government's point here: where operational information about classified activities is inherently intertwined in the evidence needed to decide the case, the very subject matter is a state secret. Moreover, Plaintiffs' observation that discovery has occurred in some cases before they were dismissed on "very subject matter" grounds, *see id.* at 21, misses the point. Whenever it is apparent, as it presently is here, that state secrets are needed to decide a case, it must be dismissed. Any other result would put privileged information at risk for no reason. In *Fitzgerald*, the "very subject matter" dismissal occurred on the eve of trial because that is when the Government first learned that experts were asked to testified about a classified Navy program and rushed in with a state secrets privilege. *See* 776 F.2d at 1238. In addition, the fact that *Clift v. United States*, 808 F. Supp. 101 (D. Conn. 1991), was "litigated for well over a decade" illustrates the error made in that case, not its merit. After waiting to see if classified information would become available, the district court dismissed that action on state secrets grounds because the central evidence was a secret from the beginning of the action. *See id.* Neither case remotely stands for the proposition that courts should wait until after discovery to decide the impact of the privilege if that impact is apparent at the outset.

"requests for admissions regarding *the facts of* MCI and Verizon's interception of Plaintiffs' call records for the Government," (3) "requests for admissions regarding *the facts of* MCI and Verizon's disclosure of Plaintiffs' communications to the Government," (4) "requests for admissions regarding *the facts of* MCI and Verizon's disclosure of Plaintiffs' call records to the Government, (5) Defendants' answers to Plaintiffs' various complaints, in order to "generat[e] admissions that would support Plaintiffs' claims," (6) "discovery [from] MCI and Verizon seeking information on the interception and disclosure of Plaintiffs' communications and records to the Government," (7) "discovery [from] MCI and Verizon on the existence of the content monitoring program," (8) confirmation from MCI and Verizon concerning "the existence of a certification authorizing monitoring of communication content," and (9) "discovery [from] MCI and Verizon on the existence of the records monitoring program, including whether either received certification authorizing monitoring of communications records." Declaration of Candace J. Morey, Docket No. 316, ¶¶ 4-15 (emphases added).

**(U)** All of this information is covered by the DNI's privilege assertion. It thus makes no sense to defer a complete decision on the state secrets issues until after discovery; the United States would just have to reassert the very same privilege in response to the discovery requests. Not only would such a process "be a waste of time and resources," *Zuckerbraun*, 935 F.2d at 548, but, more importantly, it would put the disclosure of national security information at continued risk. Plaintiffs would "have every incentive to probe as close to the core secrets" as possible in "attempt[ing] to make out a prima facie case," and such probing "would inevitably be revealing." *Farnsworth Cannon, Inc. v. Grimes*, 635 F.2d 268, 281 (4th Cir. 1980) (en banc) (per curiam). And the risk of inadvertent disclosures, which is always present in cases involving the handling of classified information, would persist. *See Sterling*, 416 F.3d at 344 ("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."); *id.* at 348 ("Inadvertent disclosure during the course of a trial—or even in camera—is precisely the sort of

risk that *Reynolds* attempts to avoid.").[20]

**(U)** This is not a case where state secrets are tangential and can be considered as discrete matters later as "individual evidentiary issues arise," Pl. Opp. at 31. The privilege assertion here covers information at the very core of Plaintiffs' claims, and the effect of the exclusion of such information on further proceedings is presently apparent. The United States' motion to dismiss or for summary judgment, moreover, has put the issue before the Court and the burden on Plaintiffs to respond. The question is ripe and appropriate for consideration at this time. The Court should consider all of the information that the United States has provided and conduct a full assessment of all foreseeable consequences of the privilege on this case.

## IV. (U) BECAUSE STATE SECRETS ARE NECESSARY FOR A FULL AND FAIR ADJUDICATION, THE CASE MUST BE DISMISSED

**(U)** Plaintiffs rest their entire case on the theory that they need only show (and will be able to prove) two sets of facts to litigate their claims: (1) the existence of a content dragnet and telephone records program, and (2) the involvement of Verizon and MCI in such programs. *See* Pl. Opp. at 32, 34. According to Plaintiffs, "proof of the programs' existence and participation in them by [the] carriers will, by definition, establish the interception and/or disclosure of Plaintiffs' communications and records." *Id.* at 34. And once interception or disclosure is established, Plaintiffs argue, any other facts are irrelevant. *See id.* at 31.

**(U)** This line of reasoning is seriously flawed and substantially oversimplifies the legal and factual issues that would be involved in a full adjudication of this case. As an initial matter, Plaintiffs are wrong that they could demonstrate the existence of any such programs or carrier

---

[20] **(U)** For example, information is put at risk every time the government creates classified submissions, posts redacted versions of such submissions on the Internet, and transports the submissions to and from the Court. Likewise, risks of inadvertent disclosures are present at every hearing in open court involving judges or attorneys who have knowledge of classified information, and every time a court writes a decision (classified or unclassified) after considering classified information.

participation absent state secrets, *see* Section II, *supra*, and that alone is enough to conclude that this litigation cannot proceed. The establishment of such facts, after all, are essential elements to every claim in this case. But even under Plaintiffs' view of the public record, additional information covered by the privilege assertion would clearly be needed to resolve their claims, starting with the fundamental issue of Plaintiffs' standing.

**A. (U) Plaintiffs Cannot Establish Standing Without State Secrets**

**(U)** Plaintiffs concede that to establish standing, they must show that "at least *one* of the named Plaintiffs had his or her communications intercepted." Pl. Opp. at 41 (emphasis in original). Yet Plaintiffs cannot establish such a fact because any information tending to confirm or deny whether they have been subject to alleged NSA activities falls squarely within the DNI's privilege assertion. *See* Public McConnell Decl. ¶ 11, 14. For the same reason, the Sixth Circuit held in *ACLU* that the state secrets privilege prevented the plaintiffs in that case from proving actual interception and dismissed the case for lack of standing. *See ACLU*, 2007 WL 1952370, at *3 ("But the plaintiffs do not — and because of the State Secrets Doctrine cannot — produce any evidence that any of their own communications have ever been intercepted by the NSA under the TSP, or without warrants."); *id.* at *5 ("Moreover, due to the State Secrets Doctrine, the proof needed either to make or negate such a showing [of actual wiretapping] is privileged, and therefore withheld from discovery or disclosure."); *id.* at *38 (Gibbons, J., concurring) ("Under any understanding of constitutional standing, the plaintiffs are ultimately prevented from establishing standing because of the state secrets privilege."); *see also* U.S. Mem. at 40-46 (discussing *Halkin*, *Ellsberg*, and other authorities).

**(U)** Plaintiffs make three arguments to avoid this fundamental problem, all of which fail. First, Plaintiffs simply allege that the NSA operates "a dragnet that sweeps in all communications and records," Pl. Opp. at 38, and argue that they can survive the United States' motion just by resting on this extremely broad allegation, *see id.* at 35-36. But our summary judgment motion puts the burden on Plaintiffs to do more than assert mere allegations; they must

actually prove their standing, or at least demonstrate how they could do so without state secrets. *See, e.g.*, *ACLU*, 2007 WL 1952370, at *37 (Gibbons, J., concurring) ("As this case was decided on the government's motion for summary judgment, the plaintiffs must set forth by affidavit or other evidence specific facts," but "plaintiffs have failed to meet this burden because there is no evidence in the record that any of the plaintiffs are personally subject to the TSP.") (citations and internal quotation marks omitted); *id.* ("On summary judgment, however, the plaintiffs' mere allegations are insufficient," and the publicly available information about the TSP "does not satisfy the plaintiffs' burden"). Because they cannot make such a showing, the case must be dismissed.[21]

**(U)** Second, Plaintiffs try to rely on purported implications from the public record to establish that the alleged activities are so broad that, by definition, Plaintiffs' communications and records must have been intercepted or disclosed. This approach is riddled with flaws. For one, the public record does not confirm or deny the existence of a telephone records program or Verizon or MCI's alleged participation, *see* Section II, *supra*, and any such information is covered by the DNI's privilege assertion. In addition, even Plaintiffs concede that the United States has *denied* the alleged content dragnet, and establishing that denial as an evidentiary matter will also require state secrets. And even if Plaintiffs could establish Verizon and MCI's participation in dragnet-type activities despite the privilege assertion, Plaintiffs would still have to show that their personal communications or records were actually intercepted or disclosed. Not even the most generous reading of the public statements on which Plaintiffs rely supports the conclusion that *every single* communication and record in the United States has been

[21] **(U)** As discussed above, *see* Section III, *supra*, allowing Plaintiffs to try to prove their standing through discovery would be pointless, because any requests for information tending to confirm or deny whether Plaintiffs were subject to alleged NSA activities would be met with the very same privilege assertion.

collected,[22] and at times Plaintiffs themselves back off from such a sweeping suggestion. *See* Pl. Opp. at 34 (arguing that there is a "high probability" that Plaintiffs' communications and records have been intercepted and disclosed). Thus, at the very least Plaintiffs must be able to determine the scope of any alleged activities (if they in fact exist), and whether the activities have been applied to them. They could not do that, however, without more detailed facts than even they claim to know.

**(U)** Finally, Plaintiffs argue that standing could be established *in camera*, even without their knowledge or participation. *See* Pl. Opp. at 41-42. This suggestion is based on the theory that the Court would only have to find, based on *ex parte* evidence from Verizon, that one of the individual Plaintiffs has standing, and that the Court could then proceed without identifying that party to anyone. The obvious problem with this approach is that the Court ultimately will have to identify who has standing and who does not. For example, if none of the Plaintiffs have standing, then the case would have to be dismissed and the denial of standing for each individual made public. If one or more Plaintiffs did have standing, however, the case could not proceed to Plaintiffs' desired end (a judgment) without identifying the individuals who were subject to interception or disclosure, and thus entitled to relief. And adding anonymous "Doe" parties would not solve the problem, *see id.* at 42 n.29, because those parties and their counsel will know their own identities and will ultimately learn, for the same reasons just described, the decision on standing. There is thus no way to adjudicate the standing question without disclosing state secrets.

---

[22] **(U)** For example, a quote in one of the news articles cited by Plaintiffs states: "It was long-distance. It was targeted on (geographic) areas of interest, places to which calls were believed to have come from al-Qaeda affiliates and from which calls were made to al-Qaeda affiliates." Pl. Ex. W at 2. While it is unclear what "[i]t" refers to, Plaintiffs claim that it is a description of the alleged call records program. *See* Pl. Opp. at 8. If that is true, and the statement could (contrary to our view) constitute a reliable and official disclosure, Plaintiffs would thus have to prove that their own records fell within any such targeted collection. *See also* Pl. Ex. W at 2 (reporting that some lawmakers were concerned that the alleged database contained "gaps" and was incomplete, though not specifying what those alleged gaps were).

**B. (U) Plaintiffs' Claims Cannot Be Adjudicated Without Confirming or Denying Verizon and MCI's Alleged Assistance**

**(U)** Plaintiffs do not dispute that this case could not proceed without information confirming or denying Verizon and MCI's alleged assistance to the NSA. The only dispute, therefore, is whether such information is protected by the state secrets privilege. For the reasons we have explained, *see* Section II, *supra*, that information is protected and thus the case must be dismissed.

**(U)** We also reiterate that the *Totten/Tenet* doctrine bars these cases as well. *See* U.S. Mem. at 26-31. In arguing the contrary, Plaintiffs largely rely on this Court's decision in *Hepting*, now on appeal, and with which we respectfully disagree. The difference between the parties on the *Totten/Tenet* doctrine comes down to whether the cases turn on which party files the lawsuit. We submit that *Totten* and *Tenet*, most fairly and reasonably construed, reflect a broader concern with the protection of confidential intelligence relationships, and that was the reason those cases were dismissed. Far from "misquoting" *Tenet*, as Plaintiffs contend, we relied upon the salient passage in which the Supreme Court held that the Court of Appeals in that case was "quite wrong" in limiting the application of *Totten* to one type of claim (breach of contract) while allowing other claims to proceed (due process, estoppel theories). *See Tenet*, 544 U.S. at 9. In explaining why *Totten* "was not so limited" to breach of contract claims, the Supreme Court's reasoning does not focus on the narrow issue of whether a party to an espionage agreement was barred by *Totten* from bringing other types of claim; rather the Court stated more broadly that "public policy forbids the maintenance of *any suit* in a court of justice, the trial of which would inevitably lead to the disclosure of matters that the law itself regards as confidential." *Id*. at 9 (original emphasis). The confidential "matter" subject to disclosure was the alleged espionage relationship. *See id*. at 11 ("The possibility that a suit may proceed and an espionage relationship may be revealed, if the state secrets privilege is not found to apply, is unacceptable[.]"). This rationale is plainly directed at the protection of espionage relationships, such as those alleged here, and reasonably applies in any suit where such relationships are at risk

of disclosure.

**C. (U) The Merits of Plaintiffs' Claims Could Not Be Adjudicated Without State Secrets**

**(U)** Plaintiffs barely respond to the United States' motion on the question of whether privileged information would be necessary to litigate the merits of their claims. *See* U.S. Mem. at 48-54. Instead, Plaintiffs simply suggest that the only relevant information is "interception or disclosure by Verizon and MCI." Pl. Opp. at 31. Such information, however, is squarely covered by the privilege assertion. And, in any event, more specific information also covered by the privilege assertion would be needed to consider the merits of Plaintiffs' claims.

**(U)** First, with respect to Plaintiffs' content dragnet claims, disproving those allegations would necessarily require demonstrating limitations on actual NSA operations, thereby revealing sensitive intelligence sources and methods. *See* U.S. Mem. at 48-51. Plaintiffs fail to grapple with this issue at all, and respond only that the limited TSP disclosures have "opened the door" to further inquiry. Pl. Opp. at 23-24. But an acknowledgment of *one* limited type of content surveillance (which is no longer operative) cannot open the door to discovery into whether *something else* is occurring.

**(U)** Second, with respect to the call records allegations, even assuming solely for the sake of argument, that the public statements could be interpreted as Plaintiffs allege *and* equated with official disclosures, any revelations from those statements would be too general to actually allow the adjudication of Plaintiffs' claims. All that such statements would arguably show (again, assuming only *arguendo* that Plaintiffs' interpretations are correct) is that (1) the NSA, at some point after September 11, 2001, collected large quantities of telephone records for an anti-terrorism purpose; (2) Verizon, despite its public statements, assisted the NSA with that collection through its wireline phone business; and (3) MCI assisted the NSA with the telephone records collection as well. Indeed, Plaintiffs themselves concede that no statements "have reveal[ed] the details of the operation of the [alleged call records] program." Pl. Opp. at 24. Thus, even if Plaintiffs' erroneous view of the public statements is accepted, Plaintiffs would

still not know and could not prove: (1) the scope of the alleged call records collection; (2) whether Plaintiffs' own individual call records were provided to the NSA as part of the alleged collection; (3) the duration of the alleged call records program and whether it is currently in operation; (4) how the alleged call records program operated (*e.g.*, were all of the call records allegedly at issue actually disclosed to the NSA or viewed by NSA analysts, or did the NSA just have potential access to a database of records); (5) the purpose of the alleged call records program; (6) the alleged program's effectiveness in detecting terrorist activity; (7) the extent of any communications, if they exist, between the Government and Verizon or MCI regarding the alleged program and its purpose, effectiveness, operation, and legal basis; and (8) whether the alleged call records collection was authorized by court order, statute, or constitutional authority, and what the factual circumstances were that allowed the invocation of any such authorities. Contrary to Plaintiffs' suggestion, all of the foregoing information would be needed for a full and fair adjudication of Plaintiffs' call records claims (assuming a program existed), starting with the fundamental question of Plaintiffs' standing and including any good faith or other statutory defenses that the Verizon/MCI Defendants might be able to raise.[23] *See* Section IV, *infra*.

**(U)** For example, the Stored Communications Act ("SCA") provides that a telecommunication carrier may divulge customer records "to a governmental entity, if the provider, in good faith, reasonably believes that an emergency involving immediate danger or death or serious physical injury to any person justifies disclosure of the information." 18 U.S.C.

[23] **(U)** Of course, if the alleged call records program did not exist, or if it did but Verizon and/or MCI did not participate, then adjudicating Plaintiffs' claims would require proving those facts, which, as the DNI explains, would detrimentally expose NSA operations, capabilities, sources and methods, and thereby help foreign adversaries evade detection. *See* Public McConnell Decl. ¶¶ 13-17; *accord* Public Alexander Decl. ¶¶ 14-19.

§ 2702(c)(4).[24] The applicability of that exception could not be litigated without discussing the operational details about any alleged records collection program, including the purpose behind the alleged activity, any particular threat it was designed to meet, how such records were used (for example, to deal with an emergency involving immediate danger of death or physical injury), and any communications between the Government and carrier (again, assuming that any such relationship existed) that would have provided the carrier's basis for a reasonable belief of emergency. Even Plaintiffs claim that the alleged program was directed at detecting and preventing terrorist attacks, *see* Master Verizon Compl. ¶¶ 142, 148, 149, and if the alleged program exists and is directed at stopping terrorism, the manner in which it may do so would be relevant to assessing the application of the section.

**(U)** In addition to that exception, other statutory provisions establish as a defense a good faith determination that the alleged provision of assistance was authorized under statutory law—in particular that such assistance could be provided without a warrant or court order under 18 U.S.C. § 2511(3). *See, e.g.* 18 U.S.C. § 2707(e)(3) (establishing good faith defense for civil actions under Stored Communications Act); *see also* 18 U.S.C. § 2520 (same defense as to violations of Wiretap Act).[25] In support of a good faith defense, the carriers would be entitled to explain any basis for their belief that assistance (if it was given) was lawful, including facts demonstrating how the activities operated and why they were needed or effective for detecting terrorist plots. And to adjudicate whether the existence of any alleged records program resulted in the divulgence of Plaintiffs' records under the statutes invoked, operational facts would have to be disclosed, including whether the NSA merely had potential access to the alleged records or whether records were actually disclosed to and personally reviewed by NSA analysts.

---

[24] **(U)** To the extent applicable, there is a similar exception to the disclosure of the content of communications under 18 U.S.C. § 2702(b)(8). *See* Master Verizon Compl. ¶¶ 202-03.

[25] **(U)** Plaintiffs' claims under these provisions are set forth at ¶¶ 214, 233-34.

**(U)** Furthermore, Plaintiffs' related Fourth and First Amendment claims both put at issue specific facts, such as whether individual interceptions of Plaintiffs' communications occurred, whether exigent circumstances warranted any actions at issue, and what specific information was actually obtained or viewed such that a legitimate privacy interest could have been invaded. *See* U.S. Mem. at 53-54; *see also Smith v. Maryland*, 442 U.S. 735, 742-46 (1979) (holding that individuals have no legitimate expectation of privacy in the numbers they dial on the telephone); *United States v. Forrester*, __ F.3d __, 2007 WL 2120271, at *6 (July 25, 2007) (amended opinion) (reaching the same conclusion regarding "to/from addresses of e-mail messages, the IP addresses of websites visited and the total amount of data transmitted to or from an account").

**(U)** Finally, another set of facts that would be implicated by any attempt to adjudicate Plaintiffs' claims on the merits is whether any of the alleged activities are ongoing, occurred only during certain periods, are no longer operative, or authorized at some point by secret court order. These issues would be relevant not only to the question of any prospective relief, but also to damages for any past alleged violation.

**(U)** In sum, litigating whether any alleged action was lawful requires a full and fair exposition of what, if anything, exactly occurred and why, as well as all possible facts and circumstances that bear upon the lawfulness of any such activities. That kind of inquiry certainly cannot be accomplished solely with reference to vague, unconfirmed, inadmissible hearsay in newspaper articles, and cannot be accomplished here without harming national security. As should be apparent, the type of discovery and fact-finding required to adjudicate a claim in federal court is far more detailed, exacting, and comprehensive than the kind of "facts" disclosed in a newspaper or magazine article, or television interview. *See, e.g.*, *El-Masri*, 479 F.3d at 308-09 ("Facts such as those furnish the general terms in which El-Masri has related his story to the press, but advancing a case in the court of public opinion, against the United States at large, is an undertaking quite different from prevailing against specific defendants in a court of law.").

**[REDACTED TEXT]**

## V. (U) CONGRESS HAS NOT ABROGATED THE STATE SECRETS PRIVILEGE IN CASES ALLEGING UNLAWFUL SURVEILLANCE.

**(U)** At the conclusion of their brief, the Plaintiffs advance a clearly erroneous argument that Section 1806(f) of FISA abrogates the state secrets privilege and "dictates" the procedure to follow whenever the Government invokes the state secrets privilege in a case involving allegations of unlawful electronic surveillance. *See* Pl. Opp. at 52. As set forth below, there is no authority that supports this argument. Indeed, Section 1806(f) serves a fundamentally different purpose: to determine the legality of surveillance that has been acknowledged by the United States. Where the "aggrieved person" (*i.e.*, someone who has been the target of surveillance) seeks discovery of FISA applications, orders, and related information, Section 1806(f) provides *the Government* with procedures on which it may rely to protect the sensitive, classified information contained in such materials. Nothing in the statute, legislative history, or applicable case law remotely suggests that these procedures can be invoked by a party seeking to discover in the first instance *whether* they have been subject to alleged unlawful surveillance. Nor does the statute or its legislative history indicate that Congress expressly sought to supplant the state secrets privilege as a means to protect against the disclosure of such information to a completely unwitting party who merely alleges surveillance. Indeed, so far as we can tell, there is not a single case in which a court has ever used this procedure to disclose whether a person had been subject to surveillance.

### A. (U) FISA Section 1806 is Inapplicable To This Case.

**(U)** The procedures set forth in Section 1806(f) generally apply where the Government intends to use the fruits of FISA surveillance "against" an "aggrieved person." *See* 50 U.S.C. § 1806(c), (e) & (f). Located within FISA's provision governing the "[u]se of information" obtained from surveillance (50 U.S.C. § 1806), the procedures of subsection (f) are limited to three situations in which the potential use of surveillance-based information in legal proceedings

against an "aggrieved person" requires a judicial determination of whether the underlying surveillance was lawful:

> (1) the Government provides notice that it "intends to enter into evidence or otherwise use or disclose" surveillance-based information in judicial or administrative proceedings against an aggrieved person, 50 U.S.C. §§ 1806(c), (d);
>
> (2) the "aggrieved person" moves in such proceedings to suppress "evidence [or information] obtained or derived from an electronic surveillance," *id.* §§ 1806(e), (f); or
>
> (3) the "aggrieved person" moves to "discover or obtain" "applications, orders, or other materials relating to electronic surveillance" or "evidence or information obtained or derived from electronic surveillance," *id.* § 1806(f).

*See also ACLU Found. v. Barr*, 952 F.2d 457, 462 (D.C. Cir. 1991).

**(U)** Each of these limitations is premised on the fact that electronic surveillance has already been disclosed. The Government's notice under § 1806(c) or (d) of its intent to use such evidence necessarily discloses the fact of surveillance. Similarly, a motion to suppress such surveillance-based evidence under § 1806(e) is made only after the Government reveals surveillance in proceedings.

**(U)** Finally, requests to "discover or obtain" evidence or information relating to or derived from surveillance are predicated on disclosed surveillance. Indeed, Congress specified that such requests must be "made by an aggrieved person," which requires the movant to have established that he was a "*target of* an electronic surveillance" or a "person whose communications or activities were *subject to* electronic surveillance." 50 U.S.C. §§ 1801(k), 1806(f) (emphases added). Moreover, the structure of Section 1806 confirms that such motions or requests are not mechanisms to discover surveillance in the first place. Section 1806 governs the Government's "[u]se of information" obtained from surveillance generally, and the specific other contexts to which Congress applied subsection (f) concern the Government's use of surveillance-based information in legal proceedings. Established canons of statutory construction thus indicate that this final category in subsection (f) is similarly limited. See *Washington Dep't of Soc. & Health Servs. v. Estate of Keffeler*, 537 U.S. 371, 384-85 (2003);

*Adams v. United States*, 420 F.3d 1049, 1053-54 (9th Cir. 2005) (where "'several items in a list shar[e] an attribute,'" this canon "'counsels in favor of interpreting the other items as possessing that attribute as well'").

**(U)** FISA's legislative history confirms that Section 1806(f) does not permit individuals to discover whether they have been subject to surveillance. Congress crafted Section 1806(f) to strike a "balance" between the aggrieved person's "ability to defend himself" against the Government's use of the legal process, and the need to protect "sensitive foreign intelligence information" from disclosure. See S. Rep. No. 95-701, at 64; cf. H.R. Conf. Rep. No. 95-1720, at 31-32 (1978) (adopting Senate's framework for Section 1806(f)). Congress thus recognized that the "need to preserve secrecy for sensitive counterintelligence sources and methods" would make "notice [of surveillance] to the surveillance target" inappropriate "*unless the fruits are to be used against him in legal proceedings*." S. Rep. No. 95-701, at 11-12 (emphasis added). And, even where a court orders information disclosed to the aggrieved person, Congress gave the Government a choice: "either disclose the material or forgo the use of the surveillance-based evidence." S. Rep. No. 95-701, at 65. That choice exists only when the Government uses such evidence as a sword. Otherwise, FISA is structured to *preserve* the confidentiality, and thus effectiveness, of intelligence-gathering. *See*, *e.g.*, 50 U.S.C. §§ 1805(a) (*ex parte* orders), 1806(j).[26]

**(U)** The D.C. Circuit's decision in *ACLU Foundation v. Barr* is instructive on this issue. The court in *Barr* held that the plaintiffs who merely alleged ongoing surveillance were not entitled to use FISA procedures to discover whether they were in fact subject to surveillance,

---

[26] **(U)** Notably, Section 1806(j), which requires disclosure to the target of certain forms of emergency surveillance, expressly provides that such notice may be withheld for "good cause." The legislative history of this provision states that "if the Government can show a likelihood that notice would compromise an ongoing investigation, or confidential sources or methods, notice should not be given." S. Rep. No. 95-604, pt. 1, at 60, 1978 U.S.C.C.A.N. 3904, 3961. This underscores that Section 1806's notice provisions are concerned with the protection of confidential information, not discovery of alleged surveillance upon mere motion in any case.

noting that "if the government is forced to admit or deny such allegations, in an answer to the complaint or otherwise, it will have disclosed sensitive information that may compromise critical foreign intelligence activities." *Id.* at 469 & n.13 ("The government makes the point, with which we agree, that under FISA it has no duty to reveal ongoing foreign intelligence surveillance").[27] Indeed, the court in *Barr* held that, in a Rule 56 summary judgment proceeding, "the government would need only assert that plaintiffs do not have sufficient evidence to carry their burden of proving ongoing surveillance . . . ." 952 F.2d at 469. The court could not have reached this result if the Plaintiffs' reading of Section 1806(f) were correct.

Under Plaintiffs' view, however, a litigant could obtain the relief requested—discovery of surveillance—in order to prove that he was an aggrieved person and was therefore entitled to discovery of the surveillance. Plaintiffs would thus transform this provision into an engine for anyone to discover whether they have been subject to surveillance. This argument turns FISA's "aggrieved person" requirement on its head, and threatens grave harm to national security because any potential target of FISA-authorized or other surveillance could force disclosure of sensitive intelligence-gathering by simply alleging, on information and belief, to be aggrieved (much as Plaintiffs have done here). Plaintiffs do not cite a single case in support of this radical theory.[28]

---

[27] **(U)** *See also In re Grand Jury Investigation*, 431 F. Supp.2d 584 (E.D. Va. 2006) (denying notice under FISA Section 1806(c) of whether grand jury witnesses had been subject to the Terrorist Surveillance Program); *In re Sealed Case*, 310 F.3d 717, 741 (For. Intel. Surv. Rev. 2002) (FISA does not require notice to a person whose communications were intercepted unless the government "intends to enter into evidence or otherwise use or disclose" such communications in a trial or other enumerated official proceedings;" otherwise "'the need to preserve secrecy for sensitive counterintelligence sources and methods justifies elimination of the notice requirement.'") (citing Senate Report 95-701, 95th Cong., 2d Sess., at 12 (1978), 1978 U.S.C.C.A.N. 3973, 3980); *In re Grand Jury Proceedings*, 856 F.2d 685, 688 (4th Cir. 1988) (grand jury witness not entitled to notice of alleged surveillance under FISA Section 1806(c)).

[28] **(U)** All of the reported cases that we have found apply Section 1806(f) where the United States or State government has sought to use evidence related to electronic surveillance

(continued...)

**(U)** Plaintiffs' assertion that the availability of the state secrets privilege in the face of Section 1806(f) would "'create[] rights which are completely illusory," *see* Pl. Opp. at 51-52, and "nullify" FISA's private remedy provisions, *see id.* at 53, is meritless. The fact that Congress has created a cause of action does not mean that other defenses that may apply in particular cases, such as claims of privilege, could not be raised. Indeed, *Reynolds* and *Kasza* demonstrate that the state secrets privilege may apply in—and lead to the dismissal of—suits brought under statutory causes of action. The creation of a cause of action says nothing about whether privileged information may be protected. And Section 1806(f) does have a clear and significant application beyond cases where the privileged fact of surveillance cannot be revealed. *See* n.28, *supra*.

**B. (U) Section 1806 Does Not Preempt the State Secrets Privilege**

**(U)** Congress could not abrogate the state secrets privilege through Section 1806(f) without (at a minimum) clearly stating its intent to do so. First, the privilege has "a firm foundation in the Constitution, in addition to its basis in the common law of evidence." *El-Masri*, 479 F.3d at 303-04 (citing *Nixon*, 418 U.S. at 710). Serious constitutional questions would arise if Section 1806(f) of FISA were read to abrogate the privilege and thereby impair the President's ability to protect vital military and intelligence secrets from public disclosure. The constitutional avoidance doctrine counsels that Section 1806(f) be construed to avoid such difficulties "unless such construction is plainly contrary to the intent of Congress." *See Edward J. DeBartolo Corp. v. Florida Gulf Coast Bldg. & Constr. Trades Council*, 485 U.S. 568, 575

---

(...continued)
in judicial proceedings and is responding to a suppression motion, or has invoked 1806(f) to protect against the unauthorized disclosure of FISA applications, orders and related information. *See, e.g., United States v. Damrah*, 412 F.3d 618, 622 (6th Cir. 2005); *United States v. Hammoud*, 381 F.3d 316, 331-32 (4th Cir. 2004), *vacated and remanded on other grounds*, 543 U.S. 1097 (2005); *United States v. Squillacote*, 221 F.3d 542, 552 (4th Cir. 2000), *cert. denied*, 532 U.S. 971 (2001); *United States v. Johnson*, 952 F.2d 565, 571-73 (1st Cir.), *cert. denied*, 506 U.S. 816 (1992); *United States v. Ott*, 827 F.2d 473, 474 (1987).

(1988). The "clear statement doctrine" similarly requires that statutes not be read to interfere with the President's powers unless Congress has made clear an intent to confront the ensuing constitutional questions. See *Armstrong v. Bush*, 924 F.2d 282, 289 (D.C. Cir. 1991).

**(U)** Second, in addition to its constitutional foundation, the state secrets privilege is deeply rooted at common law. *Kasza*, 133 F.3d at 1167. "'The common law . . . ought not to be deemed repealed, unless the language of a statute be clear and explicit for this purpose.'" *Norfolk Redevelopment & Housing Auth. v. Chesapeake & Potomac Tel. Co.*, 464 U.S. 30, 35 (1983); *see Kasza*, 133 F.3d at 1167. Nowhere in Section 1806(f) is there any indication, let alone a clear statement, that Congress had intended to restrict the applicability of the state secrets privilege in cases like this. Plaintiffs' only argument to the contrary is that Congress must have been aware of the state secrets privilege when it enacted the FISA. *See* Pl. Opp. at 51. But that is a non sequitur. Congress may have been aware of the privilege without intending to abrogate it, and Plaintiffs' argument falls well short of demonstrating a clear intent by Congress to attempt to restrict the Executive's ability to protect foreign intelligence surveillance through invocation of that privilege.

**(U)** Third, Section 6 of the National Security Agency Act of 1959 mandates that "nothing in this Act or *any other law . . . shall be construed* to require the disclosure . . . of any information with respect to the activities" of the NSA. See 50 U.S.C. § 402 note (emphasis added). This anti-disclosure provision is "absolute" (*Linder v. National Security Agency*, 94 F.3d 693, 698 (D.C. Cir. 1996)), and its "plain text unequivocally demonstrates that Congress intended to prevent" the radical interpretation of FISA that plaintiffs advance with respect to alleged surveillance activities undertaken by the NSA. *See California v. United States*, 215 F.3d 1005, 1009 n.3, 1011& n.4 (9th Cir. 2000) (construing similar text). Indeed, Section 6, as well as statutory authority directing the DNI to protect intelligence sources and methods, *see* 50 U.S.C. § 403-1(i)(1), demonstrate that the Executive Branch's assertion of the state secrets privilege in this case is directly supported by statutory law and, thus, would be at the "highest

ebb" of Presidential authority under *Youngstown*, not its lowest as Plaintiffs' assert, *see* Pl. Opp. at 49.[29]

## CONCLUSION

For the foregoing reasons, and those set forth in the United States' opening brief, the Court should uphold the state secrets and statutory privilege assertions and grant the United States' motion to dismiss or for summary judgment.

DATED: August 3, 2007

Respectfully Submitted,

PETER D. KEISLER
Assistant Attorney General, Civil Division

CARL J. NICHOLS
Deputy Assistant Attorney General

JOSEPH H. HUNT
Director, Federal Programs Branch

*s/ Anthony J. Coppolino*
ANTHONY J. COPPOLINO
Special Litigation Counsel
tony.coppolino@usdoj.gov

*s/ Andrew H. Tannenbaum*
ANDREW H. TANNENBAUM
Trial Attorney
andrew.tannenbaum@usdoj.gov
U.S. Department of Justice
Civil Division, Federal Programs Branch
20 Massachusetts Avenue, NW
Washington, D.C. 20001
Phone: (202) 514-4782/(202) 514-4263
Fax: (202) 616-8460/(202) 616-8202
*Attorneys for United States of America*

[29] **(U)** Plaintiffs' reliance on *Halpern v. United States*, 258 F.2d 36 (2d Cir. 1958), for the proposition that a statute may waive the state secrets privilege, *see* Pl. Opp. at 52, is without merit. In particular, in *Clift v. United States*, 597 F.2d 826, 829 (2d Cir. 1979), the Second Circuit revisited *Halpern* and distinguished that case in finding that the state secrets privilege was *not* waived by the Inventions Secrecy Act. *See also Clift*, 808 F. Supp. at 110 (on remand, holding that the Inventions Secrecy Act should not be interpreted to waive the state secrets privilege, because that would "turn an absolute privilege into a qualified one, which is unsupported by precedent or statute").