CINDY COHN (SBN 145997)
cindy@eff.org
LEE TIEN (SBN 148216)
KURT OPSAHL (SBN 191303)
JAMES S. TYRE (SBN 083117)
MARK RUMOLD (SBN 279060)
ANDREW CROCKER (SBN 291596)
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109
Telephone: (415) 436-9333
Fax: (415) 436-9993

RICHARD R. WIEBE (SBN 121156)
wiebe@pacbell.net
LAW OFFICE OF RICHARD R. WIEBE
One California Street, Suite 900
San Francisco, CA 94111
Telephone: (415) 433-3200
Fax: (415) 433-6382

RACHAEL E. MENY (SBN 178514)
rmeny@kvn.com
PAULA L. BLIZZARD (SBN 207920)
MICHAEL S. KWUN (SBN 198945)
AUDREY WALTON-HADLOCK (SBN 250574)
BENJAMIN W. BERKOWITZ (SBN 244441)
JUSTINA K. SESSIONS (SBN 270914)
KEKER & VAN NEST, LLP
633 Battery Street
San Francisco, CA 94111
Telephone: (415) 391-5400
Fax: (415) 397-7188

THOMAS E. MOORE III (SBN 115107)
tmoore@rroyselaw.com
ROYSE LAW FIRM, PC
1717 Embarcadero Road
Palo Alto, CA 94303
Telephone: (650) 813-9700
Fax: (650) 813-9777

ARAM ANTARAMIAN (SBN 239070)
aram@eff.org
LAW OFFICE OF ARAM ANTARAMIAN
1714 Blake Street
Berkeley, CA 94703
Telephone: (510) 289-1626

Attorneys for Plaintiffs

UNITED STATES DISTRICT COURT

FOR THE NORTHERN DISTRICT OF CALIFORNIA

CAROLYN JEWEL, TASH HEPTING, YOUNG BOON HICKS, as executrix of the estate of GREGORY HICKS, ERIK KNUTZEN and JOICE WALTON, on behalf of themselves and all others similarly situated, Plaintiffs, v. NATIONAL SECURITY AGENCY, *et al.*, Defendants.	CASE NO. 08-CV-4373-JSW **PLAINTIFFS' RESPONSES TO THE COURT'S FOUR QUESTIONS** **Hearing Date Not Yet Set** Courtroom 11, 19th Floor The Honorable Jeffrey S. White

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Rules

Legislative Materials

INTRODUCTION

Plaintiffs filed their complaint on September 18, 2008, over five years ago. To date, no defendant has answered the complaint, and the Court has blocked any discovery. Previously, the Court (per Walker, C.J.) *sua sponte* dismissed plaintiffs' action for lack of standing. ECF No. 57. Over two years ago, the Ninth Circuit reversed the dismissal and remanded for further proceedings. It found that plaintiffs "have standing to bring their statutory and constitutional claims against the government for what they describe as a communications dragnet of ordinary American citizens" "[i]n light of detailed allegations and claims of harm linking [plaintiffs] to the intercepted telephone, internet, and electronic communications." ECF No. 75; *Jewel v. NSA*, 673 F.3d 902, 905 (9th Cir. 2011). This holding is law of the case.

On remand, plaintiffs moved for partial summary judgment on the issue of whether the statutory procedure of 50 U.S.C. § 1806(f) for handling national security evidence and deciding the lawfulness of electronic surveillance applied to plaintiffs' statutory and constitutional claims. The government cross-moved to dismiss on the ground that the state secrets privilege barred this lawsuit.

The Court ruled that section 1806(f)'s "*in camera* review procedure in FISA applies and preempts the determination of evidentiary preclusion under the state secrets doctrine. Section 1806(f) of FISA displaces the state secrets privilege in cases in which electronic surveillance yields potentially sensitive evidence by providing secure procedures under which courts can consider national security evidence that the application of the state secrets privilege would otherwise summarily exclude." Amended Order at 12 (ECF No. 153).

At the September 27, 2013 Case Management Conference, the Court requested further briefing on four questions:

1. "[W]hether FISA preempts the application of the state secrets privilege to plaintiffs' constitutional claims."

2. "Must the Court follow FISA's procedural mechanisms when adjudicating the constitutional claims?"

3. "This Court requires supplemental briefing to address standing in light of the *Clapper* Court's concern about national security." The Court's reference was to the dictum in footnote 4 of *Clapper v. Amnesty International USA*, __ U.S. __, 133 S.Ct.1138, 1149 n.4 (2013), which states that in a "hypothetical disclosure proceeding" in which the government reveals whether it has targeted the plaintiff's communications, "the court's postdisclosure decision about whether to dismiss the suit for lack of standing would surely signal to the terrorist whether his name was on the list of surveillance targets."

4. "In light of the ongoing disclosures and declassification of the materials involving the government's continuing surveillance activities, the Court requires further briefing on the impact on defendant's assertion of the risks to national security presented by this case."

9/27/13 Tr. at 5:19 to 7:8 (ECF No. 164).

Plaintiffs hereby respond to the government's December 20, 2013 memorandum addressing Questions 1, 2, and 4 assigned to the government by the Court and address Question 3 assigned to plaintiffs by the Court.

None of these four questions raises any impediment to the resolution of this lawsuit on the merits, using the secure procedures of section 1806(f) if necessary. As the government concedes, the Court's holding that section 1806(f) displaces the state secrets privilege with respect to plaintiffs' statutory claims applies equally to plaintiffs' constitutional claims. The government's renewed contention that plaintiffs nonetheless must prove up their surveillance claims before the Court may use the procedures of section 1806(f) makes no sense, is contrary to the statute and its legislative history, and was rejected by the Court (per Walker, C.J.) in *In re National Security Agency Telecommunications Records Litigation (Al-Haramain)*, 595 F.Supp.2d 1077, 1085 (N.D. Cal. 2009).

The *Clapper* dictum has no application here for three independent reasons: First, the rationale of the dictum—that by ruling on a plaintiff's standing a court would reveal whether the plaintiff had been targeted for surveillance—applies only to targeted surveillance claims, not untargeted surveillance claims like those at issue here. Second, the dictum did not address section 1806(f) or its requirement that courts adjudicate the lawfulness of electronic surveillance

using national security evidence if necessary. Third, the dictum did not address circumstances like those present here where there is substantial public evidence that the plaintiffs have been subject to surveillance.

The substantial and credible public evidence supporting plaintiffs' claims—and the fact that those claims are based on mass, untargeted surveillance—also rebuts the government's claims that litigating plaintiffs' claims would endanger national security. The government has conceded the existence of the surveillance that plaintiffs challenge, and there is independent public evidence substantiating both the surveillance and AT&T's participation in it. Congress has provided section 1806(f) to protect the secrecy of any national security evidence whose consideration is necessary to deciding plaintiffs' claims. Deciding plaintiffs' claims will not reveal who the government is targeting or how it is targeting them, it will only determine the legality of the mass surveillance in which the government is concededly engaging—a question of pressing importance to millions of Americans. Plaintiffs' lawsuit should go forward.

ARGUMENT

I. Section 1806(f) Applies To Plaintiffs' Constitutional Claims Just As It Does To Plaintiffs' Statutory Claims (Question 1)

Section 1806(f) applies to plaintiffs' constitutional claims in the same manner it applies to their statutory claims: it displaces the common-law state secrets privilege and provides a secure procedure by which the Court decides "the legality of the surveillance" when that determination depends on evidence whose disclosure "would harm" national security. 50 U.S.C. § 1806(f). While section 1806(f) is an available tool for use in deciding plaintiffs' constitutional claims, whether it will be necessary to use it in deciding those claims cannot yet be determined at this early stage of the litigation, before any defendant has answered the complaint and before any discovery has been permitted.

"[T]he Government does not dispute that the Court's ruling on FISA preemption would apply equally to Plaintiffs' constitutional claims as it does to their statutory claims." Gov't Br.

at 14 (ECF No. 167). The government's concession is correct.[1]

As the Court held with respect to statutory claims, section 1806(f) displaces the common-law state secrets privilege and provides a mechanism that "permit[s] courts to determine whether any particular surveillance was lawfully authorized and executed." Amended Order at 13 (ECF No. 153). As explained at length in plaintiffs' section 1806(f) motion for summary judgment, by providing a mechanism for adjudicating claims using national security evidence that the state secrets privilege would otherwise exclude, Congress occupied the field and left no room for the state secrets privilege to operate. ECF No. 83 at 12-18; ECF No. 112 at 2-13; *see also* Amended Order at 12, 14 (ECF No. 153). In the realm of claims challenging the lawfulness of electronic surveillance, the displacement of the state secrets privilege by section 1806(f) is complete, and includes constitutional as well as statutory claims. Nothing in section 1806(f) or its legislative history carves out constitutional claims and excludes them from its scope. To the contrary, both the plain language and the legislative history of the statute affirm its application to constitutional claims.

The plain language of section 1806(f) makes no distinction between constitutional and statutory violations: it requires the Court to determine "whether the surveillance . . . was lawfully authorized and conducted"—*i.e.*, "the legality of the surveillance." 50 U.S.C. § 1806(f). Unconstitutional surveillance is just as illegal as is surveillance in violation of a statute. If it had intended to limit section 1806(f) to only a determination of statutory lawfulness, Congress could

[1] Previously, in their motion for partial summary judgment, plaintiffs specifically argued that "[s]ection 1806(f) applies to all civil claims challenging the lawfulness of electronic surveillance, whether brought under section 1810 of FISA or some other law, such as *the constitutional claims*, Wiretap Act claims, and SCA claims brought by plaintiffs here." ECF No. 83 at 17 (italics added). Plaintiffs repeated the point in their combined reply and opposition. ECF No. 112 at 6.

The government never argued that section 1806(f) is inapplicable to constitutional claims. To the contrary, the government's opposition argued that one proper use of section 1806(f) is in criminal cases where the defendants bring a suppression motion under the Fourth Amendment—a type of constitutional claim—such as in *Alderman v. United States*, 394 U.S. 165, 176 (1969). ECF No. 102 at 39. Thus, the government in its prior briefing argued that section 1806(f), in cases where it applies, applies to constitutional claims, and it is no surprise that it continues to maintain that position.

have easily done so, *e.g.*, by limiting a court's power to determining only "the legality of the surveillance under FISA, the Wiretap Act, or the Stored Communications Act." Manifestly, Congress did not. Moreover, in the 35 years since section 1806(f)'s enactment in 1978 no member of Congress has ever proposed any legislation to narrow or limit the scope of section 1806(f), even though there have been other amendments to FISA.

The legislative history confirms section 1806(f)'s broad scope. Not just section 1806(f) but the entire statutory framework of FISA of which it forms an essential part was erected by Congress to safeguard constitutional rights.[2] FISA "reconcile[s] national intelligence and counterintelligence needs with constitutional principles in a way that is consistent with both national security and individual rights." S. Rep. No. 95-701, at 16 (1978), *reprinted in* 1978 U.S.C.C.A.N. 3973, 3985.

Congress specifically intended that section 1806(f) apply to constitutional claims, noting that the court would "determine whether the surveillance was authorized and conducted in a manner which did not violate any constitutional or statutory right." S. Rep. No. 95-701, at 63 (1978), *reprinted in* 1978 U.S.C.C.A.N. 3973, 4032; *accord*, S. Rep. No. 95-604(I), at 57 (1977), *reprinted in* 1978 U.S.C.C.A.N. 3904, 3959; *ACLU Foundation of Southern California v. Barr*,

---

[2] "Congress enacted FISA to curb the problem of unchecked domestic surveillance and intelligence-gathering abuses undertaken by the executive branch in the post-World War II era." Amended Order at 12 (ECF No. 153). Congress was equally, if not more, concerned with constitutional violations as it was with statutory violations. The Church Committee concluded that the "massive record of intelligence abuses over the years" had "undermined the *constitutional* rights of citizens . . . primarily because checks and balances designed by the framers of the Constitution to assure accountability have not been applied." S. Rep. No. 94-755 (*Book II: Intelligence Activities and the Rights of Americans*), at 290, 289 (1976) (italics added). It recommended legislation to "make clear to the Executive branch that [Congress] will not condone, and does not accept, any theory of inherent or implied authority to violate the Constitution, the proposed new charters, or any other statutes." *Id*. at 297.

In enacting FISA, Congress recognized the need for statutory protections to ensure that constitutional rights are not infringed or chilled: "Also formidable—although incalculable—is the 'chilling effect' which warrantless electronic surveillance may have on the constitutional rights of those who were not targets of surveillance, but who perceived themselves, whether reasonably or unreasonably, as potential targets. Our Bill of Rights is concerned not only with direct infringements on constitutional rights, but also with government activities which effectively inhibit the exercise of these rights." S. Rep. No. 95-604(I), at 8 (1977), *reprinted in* 1978 U.S.C.C.A.N. 3904, 3909.

952 F.2d 457, 465 n.7 (D.C. Cir. 1991). Congress' decision to include constitutional claims in section 1806(f) accords with "[t]he judiciary's essential role in protecting constitutional rights" and the fundamental jurisprudential principle that constitutional claims deserve a meaningful judicial forum. *In re National Security Agency Telecommunications Records Litigation (Hepting)*, 671 F.3d 881, 899 & n.3 (9th Cir. 2011). "The federal courts remain a forum to consider the constitutionality of the wiretapping scheme and other claims, including claims for injunctive relief." *Id.*

Thus, there is no doubt that Congress intended section 1806(f) to apply to constitutional claims just as it applies to statutory claims. Nor is there any coherent reason why constitutional rights would be subject to a lesser standard of protection than statutory rights. If anything, constitutional rights are superior to and more jealously guarded than statutory rights.

There is also no coherent reason why Congress would direct the Court to use national security evidence to decide plaintiffs' statutory claims but to abstain from using the same evidence to decide plaintiffs' constitutional claims. Once national security evidence comes in pursuant to section 1806(f), it is in the case for all purposes and all claims. A contrary rule that when the Court turns to plaintiffs' constitutional claims it must put out of mind the evidence it has just used to decide their statutory claims would be absurd.

Finally, the D.C. Circuit, addressing this very question, has held that section 1806(f) applies equally to both statutory and constitutional claims: "When a district court conducts a § 1806(f) review, its task is not simply to decide whether the surveillance complied with FISA. Section 1806(f) requires the court to decide whether the surveillance was 'lawfully authorized and conducted.' The Constitution is law. Once the Attorney General invokes § 1806(f), the respondents named in that proceeding therefore must present not only their statutory but also their constitutional claims for decision." *ACLU v. Barr*, 952 F.2d at 465. Other courts have also used section 1806(f) to review constitutional challenges to surveillance. *U.S. v. Johnson*, 952 F.2d 565, 571-72 & n.4 (1st Cir. 1991). This Court should so hold as well.

II. Whether The Court Will Ultimately Need To Use Secret Evidence, And Therefore Will Need To Use The Procedures Of Section 1806(f), To Adjudicate This Lawsuit Cannot Yet Be Determined (Question 2)

None of this is to say that resort to section 1806(f) will ultimately prove necessary in this lawsuit. The issues raised by plaintiffs' claims are primarily legal in nature, given the bulk, untargeted nature of the government's surveillance. They do not turn on the details of the government's targets or the government's purpose. This lawsuit is therefore unlike a challenge to targeted surveillance, where the legality of the surveillance may turn on the factual details relating to the surveillance target and the surveillance's purpose that the government relies on in its application for an order authorizing surveillance of the target. Plaintiffs' position is that no order can lawfully authorize the mass, untargeted surveillance the government is engaging in regardless of the facts put forth to support it.

Plaintiffs' forthcoming motion for partial summary judgment on their Fourth Amendment claim is based entirely on public evidence. It may ultimately be possible, after discovery, to litigate plaintiffs' other claims solely using public evidence, especially in the wake of the cascade of recent public disclosures. To this end, plaintiffs have proposed a carefully staged discovery plan to separate public evidence from national security evidence and to defer section 1806(f) proceedings and the use of national security evidence, going down that path only if it later proves necessary. Joint CMC Statement at 17-20 (ECF No. 159). Under this discovery plan, discovery of non-classified evidence would occur first, with any proceedings under section 1806(f) deferred until a later determination of whether they are necessary. Thus, while section 1806(f) is an available tool, only if review of national security evidence is necessary to deciding plaintiffs' claims *must* the Court use section 1806(f) to adjudicate those claims.

The government resurrects its tattered "aggrieved person" argument that, should national security evidence prove essential to deciding plaintiffs' claims, section 1806(f)'s procedures cannot be used unless plaintiffs first prove their claims using non-secret evidence. This is an old argument that plaintiffs thoroughly briefed in 2012, as well as earlier in the related *Hepting* litigation and on appeal in this case and the *Hepting* case. *See* ECF No. 82 at 19-22; ECF No. 112 at 13. It is the essentially circular, and nonsensical, argument that plaintiffs cannot use section 1806(f)

proceedings in proving their case unless they have already proven their case using non-secret evidence. This Court did not adopt this argument in its order ruling that section 1806(f) applies to plaintiffs' statutory claims, and it should reject this argument again here.

Congress' purpose in defining "aggrieved person" in 50 U.S.C. § 1801(k) as a person who was the "target of" or "subject to" electronic surveillance was not to create a hurdle to the use of section 1806(f) but simply to limit the remedies against unlawful surveillance (such as the civil action of 50 U.S.C. § 1810 and the suppression motions authorized by 50 U.S.C. § 1806(e)) to those who actually participated in the intercepted communication. The term was meant only to exclude "persons, *not* parties to a communication, who may be mentioned or talked about by others," because Congress had "no intent to create a statutory right in such persons." H.R. Rep. No. 95-1283, at 66 (1978) (italics added); *see also id*. at 89-90. Nor does it make sense that Congress would have intended the term "aggrieved person" to be a barrier to use of section 1806(f), given that it is the government, not the aggrieved person, that triggers section 1806(f)'s procedures by refusing a discovery request on national security grounds.

Moreover, the government ignores the prior ruling of this Court (per Walker, C.J.) in the *Al-Haramain* litigation on this point. *In re National Security Agency Telecommunications Records Litigation (Al-Haramain)*, 595 F.Supp.2d at 1085. Rejecting the same arguments the government makes here, the Court held that "*proof* of plaintiffs' claims is not necessary at this stage." *Id*. (italics original). Instead, all that is required are "allegations [that] 'are sufficiently definite, specific, detailed, and nonconjectural, to enable the court to conclude that a substantial claim is presented.' "[3] *Id*.

Plaintiffs more than meet this standard, for they have presented not just specific and detailed allegations but record evidence showing that their communications have been intercepted

[3] Indeed, as plaintiffs have explained at length elsewhere, at the time of section 1806(f)'s enactment in 1978, the "party aggrieved" standard of 18 U.S.C. § 3504 for challenging unlawful surveillance—which the Court relied on in *Al-Haramain* in interpreting section 1806(f)'s "aggrieved person" language —required only that the party show a colorable basis for believing he or she had been subject to electronic surveillance. *See* ECF No. 112 at 12-13.

and their communications records have been obtained by the government. Plaintiffs have previously set forth this evidence for the Court (*see, e.g., Plaintiffs' FRE 1006 Summary of Voluminous Evidence*, ECF No. 113; ECF No. 116; ECF No. 173; ECF No. 174), and discuss it further in section IV below.

Equally misplaced is the government's apparent suggestion (Gov't Br. at 10:9-19 (ECF No. 167)) that under section 1806(f) it has discretion to either provide or withhold evidence for the Court's *ex parte, in camera* review, and that by withholding evidence it can block the Court from deciding the legality of the surveillance. This ignores the plain language of section 1806(f), which envisions a process in which plaintiffs have made a discovery request ("any motion or request . . . pursuant to any other statute or rule of the United States . . . to discover or obtain applications or orders or other materials relating to electronic surveillance," 50 U.S.C. § 1806(f)), and the government has asserted in response to the discovery request that disclosure of the requested information would harm national security ("if the Attorney General files an affidavit under oath that disclosure or an adversary hearing would harm the national security of the United States," *id.*). Where the government has refused discovery on national security grounds, it is mandatory that the Court review the evidence and determine the legality of the surveillance ("the United States district court . . . shall, notwithstanding any other law, . . . review in camera and ex parte the application, order, and such other materials relating to the surveillance as may be necessary," *id.*).

If instead the government does *not* assert that disclosure of the requested information would harm national security, then the Federal Rules of Civil Procedure apply and the government is obligated to respond to the discovery request in the manner that the rules provide. Withholding the evidence completely is not an option that Congress provided, and would be fundamentally inconsistent with section 1806(f)'s provision that it governs "notwithstanding any other law" and this Court's holding that "§ 1806(f) preempts application of the state secrets privilege."[4] Amended

[4] Section 1806(f) grants district courts the power to disclose classified evidence, "under appropriate security procedures and protective orders," to a party challenging unlawful surveillance "where such disclosure is necessary to make an accurate determination of the legality of the surveillance." One court has recently done so. *U.S. v. Daoud*, No. 12-CR-00723, ECF No. 92 (N.D. Ill. Jan. 29, 2014); *cf.* Gov't Br. at 10 n.6 (ECF No. 167).

Order at 11 (ECF No. 153).

Finally, 18 U.S.C. § 2712 further reinforces the conclusion that section 1806(f) controls here and that the government must follow its procedures if it refuses discovery on national security grounds. Section 2712(b)(4) mandates that, "[n]otwithstanding any other provision of law, the procedures set forth in section 106(f) [1806(f)] . . . shall be the exclusive means by which materials governed by those sections may be reviewed." Its unconditional command contains no suggestion that a plaintiff must first prove its electronic surveillance claims before section 1806(f)'s protections for national security evidence come into play.

To reiterate, plaintiffs have put forward a discovery plan which separates discovery of secret information from discovery of non-secret information, and under which section 1806(f) will come into use only if consideration of secret evidence is necessary to decide the merits of plaintiffs' claims. This lawsuit should go forward under that plan.

III. The *Clapper* Dictum Has No Application To Claims For Mass Surveillance Activities, Or To Surveillance Activities That Have Been Publicly Disclosed (Question 3)

In footnote four of *Clapper*, the Supreme Court stated in dictum that if the government were forced to disclose in a targeted-surveillance lawsuit whether a plaintiff's communications were targeted for surveillance, a terrorist could file suit and "the court's postdisclosure decision about whether to dismiss the suit for lack of standing would surely signal to the terrorist whether his name was on the list of surveillance targets." *Clapper*, 133 S.Ct. at 1149 n.4. This Court asks whether a ruling that the plaintiffs here have standing for their claims of untargeted surveillance would fall within *Clapper's* dictum and reveal who the government has targeted for surveillance. For multiple reasons of both law and fact, no such risk is present here.

A. The Rationale Of *Clapper's* Dictum Applies Only To Claims Of Targeted, Not Untargeted, Surveillance

First, deciding the *Jewel* plaintiffs' claims of *untargeted* surveillance will not reveal who the government has targeted for surveillance, because that fact is irrelevant and unnecessary to plaintiffs' claims. *Clapper* was a targeted surveillance lawsuit, not an untargeted surveillance

lawsuit like this one. *Clapper* was further limited to conjectures of possible future surveillance, unlike the evidence of past and ongoing surveillance that plaintiffs rely on here.[5] The *Clapper* plaintiffs made a facial challenge to the constitutionality of 50 U.S.C. § 1881a (section 702 of FISA), a statute that authorizes only targeted surveillance ("the targeting of persons reasonably believed to be located outside the United States to acquire foreign intelligence information," 50 U.S.C. § 1881a(a)). The *Clapper* plaintiffs alleged their future communications likely would be intercepted because they communicated with persons who were likely targets of surveillance, not because they were subject to a program of untargeted mass surveillance. 133 S.Ct. at 1142-43.

In the district court, the *Clapper* plaintiffs did not invoke section 1806(f) and did not seek any discovery either of classified or public evidence. *Amnesty International USA v. McConnell*, 646 F.Supp.2d 633, 641-42, 644 (S.D.N.Y. 2009). Instead, they contended that to prove their standing it was sufficient for them to show either that there was a probability their communications would be intercepted in the future by targeted surveillance conducted by the government or that they had expended money trying to avoid potential targeted surveillance. *Clapper*, 133 S.Ct. at 1143, 1146, 1147, 1150-51. The *Jewel* plaintiffs do not rely on either of these theories for their standing. The Supreme Court held the *Clapper* plaintiffs lacked standing under either theory because it was purely speculative whether those with whom they communicated would be targeted for surveillance.[6] *Id.* at 1143, 1148-51.

---

[5] The Ninth Circuit has recognized this crucial distinction between *Clapper* and this lawsuit. Discussing the Second Circuit's decision in *Clapper*, the Ninth Circuit distinguished the standing allegations of *Clapper* (which it referred to as *Amnesty International*) from the standing allegations of plaintiffs here: "Jewel has much stronger allegations of concrete and particularized injury than did the plaintiffs in *Amnesty International*. Whereas they anticipated or projected future government conduct, Jewel's complaint alleges past incidents of *actual* government interception of her electronic communications, a claim we accept as true." *Jewel*, 673 F.3d at 911 (italics original). The Ninth Circuit's conclusion that *Clapper* is distinguishable from this lawsuit is law of the case.

[6] More particularly, the Supreme Court held that: (1) There is no Article III standing for *future* injuries unless the future injury is "certainly impending," not merely possible. *Clapper*, 133 S.Ct. at 1147-48, 1150, 1155. (2) Actions a plaintiff has taken to avoid merely possible, but not certainly impending, future injuries do not count as present injuries-in-fact for purposes of standing. *Id*. at 1150-51, 1155.

It was in that context of targeted surveillance claims that the Supreme Court's dictum in footnote four arose—a context quite different from plaintiffs' claims here for actual untargeted surveillance, not potential future targeted surveillance as in *Clapper*. After noting that the *Clapper* plaintiffs "have no actual knowledge of the Government's § 1881a targeting practices" and "have set forth no specific facts demonstrating that the communications of their foreign contacts will be targeted," the Supreme Court discussed the possibility of a "hypothetical" disclosure proceeding in which the government revealed whether it was targeting plaintiffs' communications: "[T]his type of hypothetical disclosure proceeding would allow a terrorist (or his attorney) to determine whether he is currently under U.S. surveillance simply by filing a lawsuit challenging the Government's surveillance program. . . . [T]he court's postdisclosure decision about whether to dismiss the suit for lack of standing would surely signal to the terrorist whether his name was on the list of surveillance targets." *Clapper*, 133 S.Ct. at 1148-49 & n.4.

Unlike the *Clapper* plaintiffs, the *Jewel* plaintiffs' standing is not based on the theory that they are communicating with someone targeted for surveillance, and litigating this case will not disclose who the government has targeted for surveillance. In an untargeted mass surveillance lawsuit like this one, a finding that the plaintiff has been subjected to untargeted mass surveillance does *not* "signal to the [plaintiff] whether his name was on the list of surveillance targets." *Clapper*, 133 S.Ct. at 1149 n.4. Untargeted mass surveillance sweeps up the guilty and the innocent equally and indiscriminately, and nothing about who the government has targeted for surveillance can be deduced from the fact of untargeted mass surveillance. Only later does the government filter and search the bulk information it has collected in untargeted mass surveillance for specific information relating to the particular individuals and entities it has targeted for surveillance, but this later stage is irrelevant to plaintiffs' claims and will not be revealed by litigating plaintiffs' claims. The government's public disclosure of the telephone records bulk collection program, for example, has not revealed to any terrorist whether he is a target of surveillance. The *Clapper* court simply was not speaking to lawsuits alleging untargeted surveillance, and litigating plaintiffs' claims of untargeted mass surveillance will not reveal whether anyone, plaintiff or non-plaintiff, is a surveillance target.

Thus, the *Clapper* dictum's fundamental concern—that litigation of a plaintiff's targeted-surveillance claim would unavoidably reveal who the government is targeting for surveillance—is entirely absent here. Plaintiffs' claims do not require them to prove who the targets of the surveillance were, what keywords or selectors the government may have used later to search the information it unlawfully gathered, or what if anything the government did with the data after the mass collection occurred. All of that is simply irrelevant to plaintiffs' claims, and none of it would be revealed by a ruling on the merits of plaintiffs' claims.

B. *Clapper's* Dictum Did Not Purport To Address Section 1806(f) Or Its Provisions

Second, *Clapper's* dictum addressed a hypothetical *in camera* proceeding, not the actual procedures Congress imposed on the courts in section 1806(f). In bringing their summary judgment motion, the *Clapper* plaintiffs never asserted that section 1806(f) applied to their claims. The Supreme Court did not cite section 1806(f) and it did not examine the detailed and specific terms of section 1806(f) or whether a proceeding conducted under it would inevitably disclose whether the plaintiff was "on the list of surveillance targets." *Clapper*, 133 S.Ct. at 1149 n.4.

It is Congress that has the final say here. Congress created section 1806(f) to adjudicate the legality of surveillance while protecting national security. Congress has already weighed the balance between national security and the rule of law and has found that claims of unlawful surveillance should go forward, and where necessary should do so under the protective procedures of section 1806(f). In adopting the procedures of section 1806(f), the House-Senate Conference Committee found that its "provision for security measures and protective orders ensures adequate protection of national security interests." H.R. Conf. Rep. No. 95-1720, at 32 (1978), *reprinted in* 1978 U.S.C.C.A.N. 4048, 4061. As this Court concluded, "Congress intended to formulate a balanced legislative solution to the national security problems raised in litigation over possibly unlawful executive surveillance programs." Amended Order at 13-14 (ECF No. 153).

Congress reaffirmed its determination that claims of unlawful surveillance should go forward using section 1806(f) where necessary to protect national security evidence when it enacted 18 U.S.C. § 2712 as part of the Patriot Act in 2001. There, Congress expressly instructed

this Court to use section 1806(f) to the extent that national security evidence is at issue in plaintiffs' claims. 18 U.S.C. § 2712(b)(4) ("Notwithstanding any other provision of law, the procedures set forth in section 106(f) [50 U.S.C. § 1806(f)] . . . shall be the exclusive means by which materials governed by those sections may be reviewed."). This Court has no warrant to disregard the will of Congress and invent a "national security" exception to section 1806(f) as the government would have it do.

There is more. Even if the Court proceeds under section 1806(f) and grants a discovery request for national security evidence made by the *Jewel* plaintiffs, that too would not reveal who on list of targets because plaintiffs have no plans to seek that information in discovery. That information is not necessary to prove their claims of untargeted surveillance. An adjudication by the Court in a section 1806(f) proceeding of whether plaintiffs have been subject to untargeted mass surveillance and, if so, whether the untargeted mass surveillance is illegal will not disclose, even indirectly, who the government is targeting for surveillance. *Clapper's* concern thus will not arise here even if proceedings under section 1806(f) prove necessary.

C. *Clapper's* Dictum Did Not Address Circumstances Where Independent Public Evidence Of Surveillance Exists, As Is The Case Here

Third, *Clapper's* dictum addresses a hypothetical in which the only evidence of whether the plaintiff has been subjected to surveillance is a government disclosure in litigation of whom it is targeting for surveillance. Here, by contrast, substantial public evidence exists showing that the *Jewel* plaintiffs have been subjected to surveillance. The *Clapper* plaintiffs, who filed their lawsuit the day after 50 U.S.C. § 1881a was enacted, brought a facial challenge to that targeted-surveillance statute. They had no evidence they had actually been subjected to surveillance and did not allege any actual surveillance of themselves, only the possibility of future surveillance. *Clapper*, 133 S.Ct. at 1149 ("Respondents, however, have set forth no specific facts demonstrating that the communications of their foreign contacts will be targeted."), 1150 ("respondents can only speculate as to whether *their own communications* with their foreign contacts would be incidentally acquired" (italics original)).

The *Jewel* plaintiffs, however, have substantial non-secret evidence of actual surveillance. Eight years ago, at the very beginning of plaintiffs' legal odyssey when they filed the *Hepting* lawsuit, the Court recognized that even at that early stage plaintiffs possessed independent, unrebutted public evidence demonstrating that plaintiffs have been surveilled: "AT&T and the government have for all practical purposes already disclosed that AT&T assists the government in monitoring communication content." *Hepting v. AT&T Corp.*, 439 F.Supp.2d 974, 991-92 (N.D. Cal. 2006). "In opposing a subsequent summary judgment motion, plaintiffs could rely on many non-classified materials including present and future public disclosures of the government or AT&T on the alleged NSA programs, the AT&T documents and the supporting Klein and Marcus declarations and information gathered during discovery." *Id*. at 998. "The court further notes that the AT&T documents and the accompanying Klein and Marcus declarations provide at least some factual basis for plaintiffs' standing." *Id.* at 1001.

Since then, the public record has swollen to a torrent. The existence of this public evidence showing that plaintiffs here have been subjected to mass, untargeted surveillance (discussed further in section IV below) is an additional ground distinguishing this lawsuit from *Clapper*. Because of this public evidence, there is no meaningful argument that litigating plaintiffs' claims will endanger national security. The public, and terrorists and others the government seeks to surveil, already know by the government's own admissions and the FISC opinions that have been publicly released that the government collects everyone's call records, that it collected the metadata of everyone's Internet communications for a decade until it stopped in 2011, and that it intercepts and searches the contents of millions of Internet communications every year. Those who read the news and follow the disclosures of Edward Snowden (the authenticity of which the government has repeatedly vouched for) understand a great deal more than that. Indeed, as noted in section II above and discussed further in section IV below, because of this flood tide of public evidence this lawsuit may well be able to proceed to judgment without any disclosure of secret national security evidence by the government and without any proceedings under section 1806(f). Whether or not that proves to be the case, a judgment in plaintiffs' favor will not reveal the existence of any surveillance or the identities of any surveillance targets that are not already known.

Moreover, the government in its state secrets privilege declarations has identified numerous organizations it is targeting for surveillance, including al-Qa'ida, al-Qa'ida in the Arabian Peninsula, al-Qa'ida in Iraq (including its North American associates), al-Shabaab, al-Qa'ida in the Lands of the Islamic Maghreb, Tehrik-e Taliban Pakistan, al-Nusrah Front, Boko Haram, and al-Murabitun. ECF No. 104 at 7-10; ECF No. 168 at 12-15. Thus, it is no secret to members of those organizations that the United States has targeted them for electronic surveillance.

IV. Litigating Plaintiffs' Claims Of Untargeted Mass Surveillance Will Not Endanger National Security (Question 4)

The Court asks what impact the disclosures since June 2013 by the government, Edward Snowden, members of Congress, and the news media have had on the government's previous assertions that litigating plaintiffs' claims of mass, untargeted surveillance would endanger national security. Those disclosures further confirm that plaintiffs' claims may be litigated without endangering national security.

The recent disclosures remove entirely any ground for contending that litigating plaintiffs' claims of untargeted mass surveillance will endanger national security:

- The government has publicly admitted its bulk untargeted collecting of telephone call records, its retention of those records for five years, and its repeated searching of the entirety of those records. ECF No. 167 at 12; ECF No. 168 at ¶¶ 6-9; ECF No. 169 at ¶¶ 5-6. Indeed, the government's pretense of secrecy for litigation purposes regarding its phone records collecting has long been a fiction. The existence of this program was confirmed over six and one-half years ago by members of Congress with firsthand knowledge, including members of the Intelligence Committees. ECF No. 113 at 18-25.
- The government has publicly admitted its bulk untargeted collecting of Internet metadata from 2001 to 2011. ECF No. 167 at 12; ECF No. 168 at ¶¶ 6-9; ECF No. 169 at ¶¶ 5-6, 26.
- The government has publicly admitted its so-called "upstream" interception of the contents of communications traversing the "Internet backbone." ECF No. 169

at ¶ 29; ECF No. 174-1. It has admitted that it searches the contents of those intercepted communications. ECF No. 174-1; ECF No. 172-8 at ¶ 69.

The public record, of course, reveals much more than that. There are the Klein and Marcus declarations and accompanying documents, which almost eight years ago revealed the government's interception, searching, and collection of Internet metadata and content (the second and third bullet points above), and AT&T's participation. ECF No. 84; ECF No. 85; ECF No. 89. AT&T has verified the authenticity of the AT&T documents accompanying the Klein declaration, and the government has expressly waived any privilege in the matters addressed in the Klein and Marcus declarations. ECF No. 84; ECF No. 115. The government has never put forward any *evidence* contesting any of the facts set forth in the Klein and Marcus declarations and documents.

There are the Snowden documents, including the draft NSA Office of Inspector General's report (ECF No. 147, Ex. A) and numerous presentation slides documenting various aspects of the government's surveillance activities. The government has never contested the authenticity of those documents. It has vouched for their authenticity by charging Snowden with theft of government property, unauthorized communication of national defense information, and willful communication of classified communications intelligence information to an unauthorized person. Criminal complaint, *U.S. v. Snowden*, No. 1:13 CR 265 (CMH) (E.D. Va. June 14, 2013); *see also* ECF No. 169 at ¶ 4 ("disclosures, by a former NSA contractor, of Top Secret documents concerning certain classified NSA surveillance programs"). There are the press stories written about the Snowden documents, many of which include additional admissions and disclosures by unnamed senior government officials, telecommunications carrier officials, technical experts, and others.

There are the post-Snowden disclosures by the government in press releases; declassified FISC opinions and government submissions in FISC proceedings; official statements; congressional testimony, and statements by members of Congress. *See, e.g.*, ECF No. 144; ECF No. 147; ECF No. 174; 1/31/14 Wiebe Decl. at Exs. A to H; http://icontherecord.tumblr.com.

Nevertheless, the government contends that litigating the merits of plaintiffs' claims will harm national security. Gov't Br. at 14 (ECF No. 167). The government frames its contention as a renewed assertion of the state secrets privilege. *Id*. at 11, 13-14. As such, it is an unauthorized

motion for reconsideration and should be disregarded by the Court. *See* N.D. Cal. Local R. 7-9; 9/27/13 Tr. at 6 (ECF No. 164) (instructing the government not to "reargue or seek reconsideration of the issues already decided by the Court"). The Court has already ruled that section 1806(f) displaces the state secrets privilege with respect to plaintiffs' statutory claims. Amended Order at 2, 11-15 (ECF No. 153). The government concedes that the Court's reasoning applies equally to plaintiffs' constitutional claims as well. Gov't Br. at 7 (ECF No. 167). Thus, it is improper for the government to reassert the state secrets privilege.[7]

In any event, the government has failed to carry its burden of demonstrating that litigating plaintiffs' claims will harm national security. The starting point is that, as explained in sections I and III above, plaintiffs' untargeted-surveillance claims do not require any inquiry into or disclosure of the identities of those whom the government is targeting for surveillance. Whether plaintiffs had been *subjected to* bulk, untargeted surveillance is a question that can be answered without delving into whether plaintiffs were *targets of* surveillance. Whatever post-acquisition sifting and winnowing the government may do later is irrelevant to a plaintiff's untargeted bulk surveillance claims, and need not be disclosed by the government or reviewed by the Court to determine the lawfulness of the initial acquisition. *See, e.g., Klayman v. Obama*, ___ F.Supp.2d ___, No. CV 13-0851(RJL), 2013 WL 6571596, *17 to *25 (D.D.C. Dec. 16, 2013) (analyzing Fourth Amendment claim challenging the bulk collection of telephone call records without any need to address whom the government is targeting); *ACLU v. Clapper*, ___ F.Supp.2d ___, No. 13 CIV. 3994 WHP, 2013 WL 6819708, *20 to *22 (S.D.N.Y. Dec. 27, 2013) (same).

The next step is the recognition of the public evidence in this case establishing plaintiffs' claims, including the participation of AT&T in the surveillance. The Klein and Marcus evidence proves the bulk interception of the content and metadata of plaintiffs' AT&T Internet communications. ECF No. 84; ECF No. 85; ECF No. 89. AT&T's continuing participation in

[7] The reassertion of the state secrets privilege, even apart from its impropriety as an unauthorized motion for reconsideration, suffers from many of the same substantive and procedural defects as the government's earlier state secrets privilege assertions. *See* ECF No. 112 at 17 to 27.

Internet interception and collection was also confirmed in 2013 by the Wall Street Journal. ECF No. 174-2; *see also* ECF No. 174-4; 1/31/14 Wiebe Decl. at Ex. B. The NSA Draft OIG Report proves AT&T's participation in the bulk telephone call records program.[8] ECF No. 147, Ex. A. In addition, AT&T's participation in the bulk phone records program was first disclosed in 2005 in a *Los Angeles Times* article, was confirmed in 2006 by members of the Senate and House Intelligence Committees, and was confirmed again in 2013 by the Wall Street Journal and the Washington Post. ECF No. 116 at Exs. 36, 89; ECF No. 144 at Ex. F; 1/31/14 Wiebe Decl. at Exs. A, B, C.

Because this evidence is already in the public domain, using it to litigate plaintiffs' claims cannot cause any harm. The government's mass surveillance programs are no secret, and neither is the fact of AT&T's participation in them. Plaintiffs' claims do not turn on, and will not reveal, who the government is targeting.

Even on the limited public record that existed eight years ago, the Court in *Hepting* rejected the government's position that any confirmation of AT&T's participation would harm national security. The Court found that "AT&T and the government have for all practical purposes already disclosed that AT&T assists the government in monitoring communication content" and that "public disclosures by the government and AT&T indicate that AT&T is assisting the government

[8] The NSA Draft OIG Report describes in detail the NSA's relationship with two telecommunications companies described as "Company A" and "Company B" in the report. *See* Draft OIG Report at 27-29, 33-34 (ECF No. 147, Ex. A). Only Companies A and B participated in all facets of the NSA's domestic surveillance operation—the interception of both telephone call records and Internet content and metadata—from the inception of the NSA's surveillance program. *Id*. at 33-34. The NSA's relationship with these two companies are among NSA's "most productive," enabling NSA access to large volumes of communications "transiting the United States through fiber-optic cables, gateway switches, and data networks." *Id*. at 28-29. Company A and Company B were the two largest providers of international telephone calls into and out of the United States. *Id.* at 27. FCC records confirm that AT&T and Verizon (formerly MCI/Worldcom) were the country's two largest international telephone call providers at that time. Wireline Competition Bureau, FCC, 1999 International Telecommunications Data at 33 fig. 9 (Dec. 2000), *available at*: http://transition.fcc.gov/Bureaus/Common_Carrier/Reports/FCC-State_Link/Intl/4361-f99.pdf. *See also* ECF No. 144 at Ex. A (confirming Verizon's participation in the bulk phone records program); 1/31/14 Wiebe Decl. at Ex. D (same).

to implement some kind of surveillance program." *Hepting*, 439 F.Supp.2d at 991-92, 994. Accordingly, the Court held that "[b]ecause of the public disclosures by the government and AT&T, the court cannot conclude that merely maintaining this action creates a 'reasonable danger' of harming national security." *Id*. at 994. Today's much richer record compels the same conclusion.

In addition, the government now permits telecommunications providers like AT&T to reveal that they are subject to FISA surveillance orders. 1/31/14 Wiebe Decl. at Ex. E. It is inconsistent for the government to maintain in this litigation that disclosing the fact of a telecommunication provider's participation in the surveillance at issue here would "lead to exceptionally grave damage to the national security" (Gov't Br. at 14 (ECF No. 167); *accord* ECF No. 168 at ¶ 42) when it permits the provider itself to disclose the fact of its participation whenever the provider wants to. Many providers are already making these disclosures.

Moreover, the government has made no showing that the consequences of a credible and substantiated public disclosure of surveillance activities vary depending on whether or not those disclosures are officially admitted by the government on the record. Once a credible public disclosure has occurred, the horse is out of the barn, regardless of whether the Executive blesses it with an official confirmation. The government offers no evidence that terrorists disregard published information regarding the government's surveillance activities unless it comes with a government seal of authenticity. News organizations of great integrity and well-established track records of accuracy in intelligence reporting, like the New York Times, the Washington Post, the Wall Street Journal, the Guardian, and USA Today have made repeated reports over the past eight years disclosing numerous aspects of the surveillance activities at issue in these lawsuits. In response, foreign governments, private corporations, and millions of people around the world have taken steps to secure their communications from government surveillance.

Indeed, Google, Yahoo, Microsoft, Facebook, and other technology and communications companies fear they will face a worldwide consumer backlash that will substantially harm their businesses. 1/31/14 Wiebe Decl. at Exs. F, G. Google, Yahoo, and Microsoft have all taken steps to encrypt and otherwise secure email and other data on the services and networks they operate

from government interception. *Id*. at Ex. H. And Chancellor Angela Merkel of Germany did not wait for an official admission that the United States had tapped her phone since 2002 and had conducted other surveillance directed at Germany before taking action in response to those disclosures. Agence France-Presse, *Angela Merkel rebukes US and Britain over NSA surveillance*, Telegraph (Jan. 29, 2014);[9] Ian Traynor, *et al.*, *Angela Merkel's call to Obama: are you bugging my mobile phone?*, Guardian (Oct. 23, 2013).[10] If ordinary consumers around the world with no unlawful activity to hide are taking steps to protect their privacy because of disclosures in the press regarding the government's surveillance activities, it is unreasonable to believe that a terrorist with much more to lose does not give those disclosures equal if not more credence. As the *Hepting* Court found, "AT&T's assistance in national security surveillance is hardly the kind of 'secret' . . . that a potential terrorist would fail to anticipate." *Hepting*, 439 F.Supp.2d at 993.

Finally, it is Congress and not the Executive that has the last word here. By creating causes of action for unlawful surveillance and the protective procedures of section 1806(f), Congress has determined and directed that electronic surveillance shall occur only under the rule of law, and shall be subject to judicial review for lawfulness under the Constitution and statutes of the United States in adversary proceedings in the district courts. "In the surveillance statutes, by granting a judicial avenue of relief, Congress specifically envisioned plaintiffs challenging government surveillance under this statutory constellation." *Jewel*, 673 F.3d at 913.

CONCLUSION

The Court should hold that section 1806(f) applies to plaintiffs' constitutional claims as well as to their non-constitutional claims. The *Clapper* dictum has no application here because it is limited to targeted surveillance claims unlike plaintiffs' untargeted surveillance claims and because litigating plaintiffs' claims will not reveal who is "on the list of surveillance targets." *Clapper*, 133

[9] *Available at* http://www.telegraph.co.uk/news/worldnews/europe/germany/10604664/Angela-Merkel-rebukes-US-and-Britain-over-NSA-surveillance.html.

[10] *Available at* http://www.theguardian.com/world/2013/oct/23/us-monitored-angela-merkel-german.

S.Ct. at 1149 n.4. Finally, the new evidence revealed since June 2013 further confirms and corroborates plaintiffs' prior evidence and further demonstrates that litigating the legality of these publicly known surveillance activities will not endanger national security.

But that is not all. This Court should also act decisively to move these proceedings forward speedily to a final judgment on the merits. Over five years since this action was filed, and over two years since the Ninth Circuit's remand, no defendant has answered the complaint and the Court has barred all discovery, even into concededly non-secret matters. In the meantime, the daily violation of plaintiffs' rights continues unabated. It is time for the delay to end. Plaintiffs are entitled like any other litigants to have their case progress forward to judgment: discovery should open; the complaint should be answered; a case schedule and trial date should be set. Whatever final judgment this Court issues will doubtless be only the first word, not the last word, on the subject, and will be followed by years of appellate proceedings. It is time to move forward on that journey.

DATE: January 31, 2014

Respectfully submitted,

s/ Richard R. Wiebe
Richard R. Wiebe

CINDY COHN
LEE TIEN
KURT OPSAHL
JAMES S. TYRE
MARK RUMOLD
ANDREW CROCKER
ELECTRONIC FRONTIER FOUNDATION

RICHARD R. WIEBE
LAW OFFICE OF RICHARD R. WIEBE

THOMAS E. MOORE III
ROYSE LAW FIRM, PC

RACHAEL E. MENY
PAULA L. BLIZZARD
MICHAEL S. KWUN
AUDREY WALTON-HADLOCK
BENJAMIN W. BERKOWITZ
JUSTINA K. SESSIONS
KEKER & VAN NEST LLP

ARAM ANTARAMIAN
LAW OFFICE OF ARAM ANTARAMIAN

Attorneys for Plaintiffs