

UNITED STATES
FOREIGN INTELLIGENCE SURVEILLANCE COURT
WASHINGTON, D.C.

U.S. FOREIGN
INTELLIGENCE
SURVEILLANCE COURT

2014 APR -2 PM 4:55

LEE ANN FLYNN HALL
CLERK OF COURT

IN RE APPLICATION OF THE FEDERAL
BUREAU OF INVESTIGATION FOR AN
ORDER REQUIRING THE PRODUCTION
OF TANGIBLE THINGS

Docket No. BR 14-01

**RESPONSE OF THE UNITED STATES OF AMERICA TO THE
COURT'S MARCH 21, 2014, OPINION AND ORDER RE: MOTION
OF PLAINTIFFS IN *JEWEL V. NSA* AND *FIRST UNITARIAN
CHURCH V. NSA*, BOTH PENDING IN THE UNITED STATES
DISTRICT COURT FOR THE NORTHERN DISTRICT OF
CALIFORNIA, FOR LEAVE TO CORRECT THE RECORD**

The United States respectfully submits this filing pursuant to the Court's Opinion and Order issued in the above-captioned matter on March 21, 2014 ("March 21 Order"), which directed the Government to make a filing pursuant to Foreign Intelligence Surveillance Court (FISC) Rule of Procedure 13(a),¹ and explain why it failed to notify this Court during its consideration of the Government's Motion for Second Amendment to Primary Order of preservation orders issued in two lawsuits, *Jewel v. NSA*, No. 08-cv-4373 (N.D. Cal.), and *Shubert v. Obama*, No. 07-cv-0693 (N.D. Cal.), and of the plaintiffs' understanding of the scope of those orders, following the Government's receipt of plaintiffs' counsel's February 26, 2014, email.

Based upon the nature of the claims made in *Jewel* and *Shubert*, which the Government has always understood to be limited to certain presidentially authorized intelligence collection

¹ FISC Rule of Procedure 13(a), Correction of Material Facts, provides in relevant part that, "[i]f the government discovers that a submission to the Court contained a misstatement or omission of material fact, the government, in writing, must immediately inform the Judge to whom the submission was made of:
(1) the misstatement or omission;
(2) any necessary correction;
(3) the facts and circumstances relevant to the misstatement or omission."

activities outside FISA, the Government did not identify those lawsuits, nor the preservation orders issued therein, in its Motion for Second Amendment to Primary Order filed in the above-captioned Docket number on February 25, 2014. For the same reasons, the Government did not notify this Court of its receipt of plaintiffs' counsel's February 26, 2014, e-mail. With the benefit of hindsight, the Government recognizes that upon receipt of plaintiffs' counsel's e-mail, it should have made this Court aware of those preservation orders and of the plaintiffs' disagreement as to their scope as relevant to the Court's consideration of the Government's motion and regrets its omission. The Government respectfully submits that in light of this submission, and this Court's Opinion and Order dated March 12, 2014, granting the Government's motion for temporary relief from the destruction requirement in subsection (3)E of the Court's Primary Order, no additional corrective action on the part of the Government or this Court is necessary. The facts and circumstances relevant to the Government's omission are set out below.

The Government takes its preservation obligations with the utmost seriousness, as it does its duty of candor to the Court, particularly in the setting of *ex parte* proceedings. As explained further below, it was not the Government's intention to omit information that it believed this Court would find relevant and material to its consideration of the Government's Motion for Second Amendment to Primary Order. In light of this Court's rulings on March 7 and 21 and the reasoning contained therein, the Government understands why this Court would have considered the *Jewel* plaintiffs' recently-expressed views regarding the scope of the preservation orders in *Jewel* and *Shubert* as material to its consideration of the Government's motion. The Government sincerely regrets not having brought these matters to the Court's attention prior to its March 7, 2014, ruling and assures the Court that it will apply utmost attention to its submissions in this and all other matters before this Court.

On February 25, 2014, the Government filed its Motion for Second Amendment to Primary Order. In the Motion, the Government requested that this Court amend minimization procedures related to the destruction of metadata acquired pursuant to authority of this Court so that the information could be maintained under strict conditions, for the limited purpose of ensuring that the Government continues to comply fully with its preservation obligations related to certain identified civil litigation. The cases that the Government listed in its February 25 Motion were all filed after last year's unauthorized public disclosures concerning the collection of telephony metadata pursuant to FISA authority, and all challenge the lawfulness of the collection of telephony metadata pursuant to this Court's authorization. Motion for Second Amendment at 3-5;² *see, e.g., American Civil Liberties Union v. Clapper*, No. 13-cv-3994 (WHP) (S.D.N.Y.), Complaint ¶ 1 (ECF No. 1) ("This lawsuit challenges the government's dragnet acquisition of Plaintiffs' telephone records under Section 215 of the Patriot Act, 50 U.S.C. § 1861.").

The Government did not notify the Court of *Jewel* and *Shubert* in the Motion because the Government has always understood those matters to challenge certain presidentially authorized intelligence collection activities and not metadata subsequently obtained pursuant to orders issued by this Court under FISA, and because the preservation issues in those cases had been previously addressed before the district court in which those matters are pending. *Jewel* and *Shubert*, filed in 2008 and 2007, respectively, challenge particular NSA intelligence activities authorized by President Bush after the September 11, 2001, terrorist attacks without statutory or

² Known active civil cases challenging bulk telephony metadata collection under FISC orders pursuant to FISA as unauthorized by statute and/or unconstitutional are those listed in the Motion for Second Amendment. In an additional *pro se* case, *Ndiaye v. Baker*, No. 13-cv-1701 (D. Md.), the plaintiff alleges collection of metadata pertaining to his telephone calls under FISA, among numerous other alleged acts by federal and local officials, as part of a scheme to persecute and harass him because of his ethnicity and religion. No preservation order has been entered in *Ndiaye* and the plaintiff has not expressed a view to the Government regarding preservation.

judicial authorization (i.e., the Terrorist Surveillance Program (TSP), and the Internet and telephony metadata programs).³ The *Jewel* plaintiffs stated in 2008 when they filed their complaint and asked that it be related to *Hepting v. AT&T* (a precursor to *Shubert*), “both cases allege the same facts: that in 2001 the *President authorized* a program of domestic surveillance *without court approval or other lawful authorization*, and that through this Program, the government illegally obtains and continues to obtain with AT&T’s assistance the contents of Plaintiffs’ and class members’ telephone and internet communications, as well as records concerning those communications.” Admin. Motion by Plaintiffs To Consider Whether Cases Should be Related at 3 (*Jewel* ECF No. 7) (emphasis added) (attached hereto as Exhibit A).⁴

³ The Government’s recent filing before the Northern District of California regarding its preservation obligations in cases before that court cites various portions of the *Jewel* and *Shubert* complaints that made clear to the Government that they challenge presidentially-authorized, non-court-authorized, programs. See, e.g., *Jewel* Complaint (attached as Exhibit B to Plaintiffs’ Motion for Leave to Correct the Record) ¶ 39 (President Bush “authoriz[ed] ‘a range of surveillance activities . . . without statutory authorization or court approval, including electronic surveillance of Americans’ telephone and Internet communications (the ‘Program’)”, ¶ 76 (“Defendants’ above-described acquisition in cooperation with AT&T of . . . communications content and non-content information is done without judicial, statutory, or other lawful authorization, in violation of statutory and constitutional limitations, and in excess of statutory and constitutional authority.”), ¶ 92 (“Defendants’ above-described solicitation of the disclosure by AT&T of . . . communications records . . . is done without judicial, statutory, or other lawful authorization, in violation of statutory and constitutional limitations, and in excess of statutory and constitutional authority.”), ¶¶ 110, 120, 129, 138 (“Defendants have [acquired] . . . contents of communications, and records pertaining to . . . communications . . . without judicial, statutory, or other lawful authorization, in violation of statutory and constitutional limitations, and in excess of statutory and constitutional authority.”); *Shubert* Second Amended Complaint (MDL ECF No. 771) (attached hereto as Exhibit B) ¶ 2 (“Without the approval of Congress, without the approval of any court, and without notice to the American people, President George W. Bush authorized a secret program to spy upon millions of innocent Americans, including the named plaintiffs.”), ¶ 9 (“This class action is brought on behalf of all present and future United States persons who have been or will be subject to electronic surveillance by the National Security Agency without a search warrant, a court order, or other lawful authorization since September 12, 2001.”), ¶ 55 (“Although it is true that federal law requires law enforcement officers to get permission from a federal judge to wiretap, track, or search, President Bush secretly authorized a Spying Program that did none of those things.”), ¶ 66 (“The Program admittedly operates ‘in lieu of’ court orders or other judicial authorization . . .”), ¶ 93 (“Prior to its initiation, defendants never sought authorization from the FISA Court to conduct the Spying Program.”). The district court has set a further briefing schedule to assess the Government’s compliance with the preservation order in *Jewel*.

⁴ *Hepting* is the lead case in the Multidistrict Litigation (MDL) proceeding in the Northern District of California (*In re NSA Telecommunications Records Litigation Multi-District Litigation* (designated as 3:06-md-1791-VRW)), which includes *Shubert*. *Hepting* and the other MDL cases (including *Shubert*) concern activity authorized by the President, without court approval. Among other things, these suits were brought against telecommunications companies (as opposed to the Government), and such companies are statutorily immune from suit for providing assistance to the Government pursuant to court order.

In 2007, the Government informed the district court in a then-classified submission (prior to the entry of the MDL preservation order, upon which the *Jewel* preservation order was based) that the Government did not understand the MDL proceedings to challenge FISC-authorized programs: “Because Plaintiffs have not challenged activities occurring pursuant to an order of the FISC, this declaration does not address information collected pursuant to such an authorization or any retention policies associated therewith.” Declassified Declaration of National Security Agency ¶ 12 n.4.⁵ (attached hereto as Exhibit C). In the same 2007 submission, consistent with the Government’s stated view that FISC-authorized collections were not at issue, the Government informed the district court that it was preserving a range of documents and information concerning only the presidentially-authorized activities at issue in the plaintiffs’ complaints. *See* Declass. NSA Decl. ¶¶ 6, 12-13, 16, 18-28. Thereafter, the court issued a preservation order that directed the parties to preserve “relevant” evidence that was “reasonably anticipated to be subject to discovery,” without instructing the Government then, or at any other time, that its understanding of its preservation obligations was erroneous. Nov. 6, 2007 Preservation Order (MDL ECF No. 393). An identical order was issued in *Jewel*, on stipulation by the parties, in 2009. (*Jewel* ECF No. 50).⁶

A day after the Government filed its Motion for Second Amendment with this Court on February 25, 2014, counsel for the *Jewel* plaintiffs sent an email to Civil Division counsel representing the Government in *Jewel*, suggesting that the preservation orders in *Jewel* and *Shubert* required the Government to preserve telephony metadata acquired under FISA. For the

⁵ A classified submission was necessary at that time because the existence of the presidentially-authorized program was classified and remained so until December 2013.

⁶ Consistent with the Government’s understanding of these orders in *Jewel* and *Shubert*, until the district court’s March 10, 2014, temporary restraining order and the subsequent March 12, 2014, order of this Court, the Government has complied with this Court’s requirements that metadata obtained by the NSA under Section 215 authority be destroyed no later than five years after their collection.

reasons set forth above, and as the Government has explained to the district court, it views that position as irreconcilable with the express allegations of the *Jewel* and *Shubert* complaints and the long course of litigation in both cases. Because the Government's Motion for Second Amendment already had sought relief from this Court based on a list of cases in which the parties expressly challenge the NSA's bulk collection of BR metadata pursuant to FISC authorization, *see* Motion for Second Amendment at 3-5, counsel did not appreciate – even after receiving the email from plaintiffs' counsel in *Jewel* – that it would be important to notify this Court about *Jewel* and *Shubert* or the email from counsel for the *Jewel* plaintiffs about those cases with which the Government disagreed. Rather, counsel viewed any potential dispute about the scope of the *Jewel* and *Shubert* preservation orders as a matter to be resolved, if possible, by the parties to those cases (through a potential unclassified explanation to plaintiffs' counsel) or, failing that, by the district court.⁷ In other words, the Government did not recognize a need to identify to this Court preservation orders issued in litigation that was not believed to be pertinent to the retention of BR metadata collected under authority of this Court, and which the Government had never treated as applicable to such metadata.

Accordingly, counsel responded to counsel for the *Jewel* plaintiffs, by email dated February 28, 2014, that the *Jewel* and *Shubert* matters presented a separate issue, and that they would discuss further with counsel for the *Jewel* plaintiffs after consultation with client agencies about what unclassified information could be provided to plaintiffs' counsel about the preservation effort in *Jewel*. In particular, the request in its February 28 email that counsel for the *Jewel* plaintiffs “forbear from filing anything with the FISC, or [the district court], until we

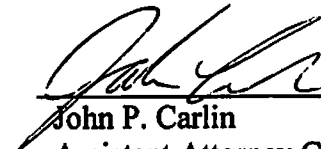
⁷ For these reasons, counsel did not think to forward the email from *Jewel* Plaintiffs' counsel to the attorneys with primary responsibility for interaction with this Court before the Court ruled on the Motion for Second Amendment. The Department wishes to assure the Court that it has always endeavored to maintain close coordination within the Department regarding civil litigation matters that involve proceedings before this Court, and will take even greater care to do so in the future.

have further opportunity to confer” was a good faith attempt to avoid unnecessary motions practice in the event that the issue could be worked out among the parties through the Government’s provision of an unclassified explanation concerning its preservation in *Jewel* and *Shubert*. Accordingly, the Government did not bring the *Jewel* plaintiffs’ February 25 email to this Court’s attention.

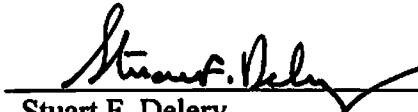
The Government’s paramount objective in its recent filings with this Court and the district courts has been to comply with its preservation obligations in civil litigation and to obtain guidance about its obligations regarding the metadata obtained pursuant to orders of this Court. The Government now appreciates that the Court would have found the *Jewel* plaintiffs’ recently-expressed views on the *Jewel* and *Shubert* preservation orders to be relevant to its consideration of the Government’s Motion for Second Amendment. As noted above, the Government sincerely regrets not apprising the Court of these matters before its March 7 ruling and assures the Court that it will apply utmost attention and coordination in its submissions in this and all other matters before this Court.

Dated: April 2, 2014

Respectfully submitted,



John P. Carlin
Assistant Attorney General
National Security Division



Stuart F. Delery
Assistant Attorney General
Civil Division

United States Department of Justice

ELECTRONIC FRONTIER FOUNDATION
CINDY COHN (145997)
cindy@eff.org
LEE TIEN (148216)
KURT OPSAHL (191303)
KEVIN S. BANKSTON (217026)
JAMES S. TYRE (083117)
454 Shotwell Street
San Francisco, CA 94110
Telephone: 415/436-9333; Fax: 415/436-9993

THOMAS E. MOORE III (115107)
tmoore@moorelawteam.com
THE MOORE LAW GROUP
228 Hamilton Avenue, 3rd Floor
Palo Alto, CA 94301
Telephone: 650/798-5352; Fax: 650/798-5001

RICHARD R. WIEBE (121156)
wiebe@pacbell.net
LAW OFFICE OF RICHARD R. WIEBE
425 California Street, Suite 2025
San Francisco, CA 94104
Telephone: 415/433-3200; Fax: 415/433-6382

Attorneys for Plaintiffs

UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF CALIFORNIA

TASH HEPTING, GREGORY HICKS,
CAROLYN JEWEL and ERIK KNUTZEN, on
behalf of themselves and all others similarly
situated,

Plaintiffs,

vs.

AT&T CORP., *et al.*,

Defendants.

CASE NO. C-06-0672-VRW

**ADMINISTRATIVE MOTION BY
PLAINTIFFS TO CONSIDER WHETHER
CASES SHOULD BE RELATED;
DECLARATION OF KEVIN S.
BANKSTON**

**[PROPOSED ORDER FILED
CONCURRENTLY]**

CAROLYN JEWEL, TASH HEPTING,
GREGORY HICKS, ERIK KNUTZEN and
JOICE WALTON, on behalf of themselves and
all others similarly situated,

Plaintiffs,

vs.

NATIONAL SECURITY AGENCY, *et al.*,

Defendants.

CASE NO. C-08-4373-CRB

[N.D. CAL Civ. L.R. 3-12, 7-11]

1 TO ALL PARTIES AND TO THEIR RESPECTIVE ATTORNEYS OF RECORD:

2 Pursuant to Civil Local Rules 3-12 and 7-11, Plaintiffs hereby move the Court for an Order
3 relating *Jewel, et al., v. NSA, et al.*, No. C-08-4373-CRB (hereinafter simply "*Jewel*") to *Hepting,*
4 *et al. v. AT&T Corp. et al.*, No. C-06-0672-VRW (hereinafter simply "*Hepting*").

5 **APPLICABLE RULE**

6 Civil Local Rule 3-12 provides, in pertinent part: "An action is related to another when:
7 (1) The actions concern substantially the same parties, property, transaction or event; and
8 (2) It appears likely that there will be an unduly burdensome duplication of labor and expense or
9 conflicting results if the cases are conducted before different Judges."

10 **THE RELATIONSHIP BETWEEN JEWEL AND HEPTING**

11 On September 18, 2008, all four of the named Plaintiffs in *Hepting*, along with a fifth
12 AT&T customer, Joice Walton, filed a complaint in the U.S. District Court for the Northern
13 District of California in San Francisco. That complaint seeks damages on behalf of the named
14 Plaintiffs, and equitable relief for a class of AT&T customers, against the U.S. government and its
15 agencies, including the National Security Agency, as well as a number of current and former
16 government officials in their official and/or personal capacities. As in *Hepting*, the Plaintiffs in
17 this pending case, *Jewel*, allege that AT&T and the government have illegally collaborated in a
18 program of surveillance of Plaintiffs' and class members telephone and internet communications
19 and communications records ("the Program"), in violation of, *inter alia*, the U.S. Constitution, the
20 Foreign Intelligence Surveillance Act ("FISA"), and the Electronic Communications Privacy Act
21 ("ECPA"). *Hepting* originally was assigned to, and is still pending before, Chief Judge Vaughn R.
22 Walker; *Jewel* has been assigned to Judge Charles R. Breyer.

23 *Jewel* and *Hepting* concern substantially the same parties. As already noted, all four named
24 Plaintiffs in *Hepting* are also named Plaintiffs in *Jewel*; the Electronic Frontier Foundation serves
25 as lead counsel for the Plaintiffs in both cases. Furthermore, the definition of the *Jewel* class is
26 identical to the definition of the *Hepting* Nationwide Class:

27 All individuals in the United States that are current residential subscribers or
28 customers of AT&T's telephone services or Internet services, or that were

1 residential telephone or Internet subscribers or customers at any time after
2 September 2001.¹

3 *Hepting* named two AT&T entities as Defendants, while *Jewel* is exclusively against the United
4 States, its agencies, and current and former U.S. government officials. However, the United States
5 has intervened in *Hepting*, and has been an extremely active participant in that case. And although
6 Plaintiffs have been advised by the Department of Justice ("DOJ") that attorneys in the
7 Constitutional Torts section of the DOJ will represent individuals sued in their personal capacity in
8 *Jewel*, it appears that the same Department of Justice attorneys representing the United States in
9 *Hepting* will also represent the United States and its agencies and offices in *Jewel*.

10 In addition to concerning substantially the same parties, *Jewel* and *Hepting* concern
11 substantially the same transactions and events. In particular, both cases allege the same facts: that
12 in 2001 the President authorized a program of domestic surveillance without court approval or
13 other lawful authorization, and that through this Program, the government illegally obtained and
14 continues to obtain with AT&T's assistance the contents of Plaintiffs' and class members'
15 telephone and Internet communications, as well as records concerning those communications.
16 Discovery related to those allegations and the findings of fact required in both cases are therefore
17 also substantially the same, leading to unduly burdensome duplication of labor and expense or
18 conflicting results if the cases are conducted before different judges.

19 Furthermore, although the specific counts asserted in *Hepting* against the AT&T
20 Defendants are not strictly identical to those against the government and its officials in *Jewel*, they
21 do raise identical legal questions, *i.e.* and *e.g.*, whether the Program violated or violates Plaintiffs'
22 rights under the U.S. Constitution, FISA and ECPA. Litigating those legal questions before
23 different judges, as with the factual questions, will undoubtedly lead to unduly burdensome
24 duplication of labor and expense by both Plaintiffs and the government, and would threaten to
25 generate conflicting results.

26 ¹ Although the same in substance, the class definition in *Jewel* varies slightly in form from the
27 *Hepting* Nationwide Class definition: Because *Hepting* named AT&T entities as Defendants, while
28 *Jewel* does not, the *Hepting* definition refers to customers of "Defendants," while the definition in
Jewel refers to customers of "AT&T." Additionally, *Hepting* includes a separate California Class
not included in *Jewel*.

As explained in more detail in the attached Declaration of Kevin S. Bankston, and as required by Civil Local Rule 7-11(a), counsel for Plaintiffs in both *Hepting* and *Jewel* have attempted but failed to secure a stipulation from counsel for the Government and government Defendants in *Hepting* and *Jewel*, for AT&T in *Hepting*, and for the personal capacity Defendants in *Jewel*. However, as detailed in the Bankston declaration, neither the Government nor AT&T oppose this motion. Counsel for the personal capacity Defendants in *Jewel* has indicated that because those Defendants have not yet been served with the *Jewel* complaint, their consent is irrelevant for this motion.

The parties, transactions and events in *Hepting* and *Jewel* are substantially the same, and there is a substantial risk of unduly burdensome litigation, and, more important, of conflicting results, if *Jewel* is not related to *Hepting*. Plaintiffs therefore respectfully submit that *Jewel* can and should be related to *Hepting* pursuant to Civil Local Rule 3-12. Plaintiffs further direct the Court's attention to Rule 7.5(a) of the Rules of Procedure of the Judicial Panel on Multidistrict Litigation. That rule provides that the assignment of potential "tag-along actions" such as *Jewel* to this court as a part of *In re National Security Agency Telecommunications Records Litigation*, MDL No. M:06-cv-01791-VRW (a proceeding that also includes *Hepting*) may be accomplished without any action on the part of the Panel on Multidistrict Litigation, and Plaintiffs respectfully ask for such assignment here.

DATED: October 21, 2008

By /s/
ELECTRONIC FRONTIER FOUNDATION
CINDY COHN
LEE TIEN
KURT OPSAHL
KEVIN S. BANKSTON
JAMES S. TYRE

1 454 Shotwell Street
2 San Francisco, CA 94110
3 Telephone: 415/436-9333
4 415/436-9993 (fax)

5 RICHARD R. WIEBE (121156)
6 LAW OFFICE OF RICHARD R. WIEBE
7 425 California Street, Suite 2025
8 San Francisco, CA 94104
9 Telephone: (415) 433-3200
10 Facsimile: (415) 433-6382

11 THOMAS E. MOORE III (115107)
12 THE MOORE LAW GROUP
13 228 Hamilton Avenue, 3rd Floor
14 Palo Alto, CA 94301
15 Telephone: (650) 798-5352
16 Facsimile: (650) 798-5001

17
18 Attorneys for Plaintiffs
19
20
21
22
23
24
25
26
27
28

DECLARATION OF KEVIN BANKSTON

I, KEVIN S. BANKSTON, declare and state:

1. On Wednesday, October 1, 2008, I was informed by Plaintiffs' counsel and Electronic Frontier Foundation (EFF) Legal Director Cindy Cohn that she had spoken that morning with counsel for the government Defendants, Anthony Coppolino of the U.S. Department of Justice's Civil Division, who indicated that the government would not oppose relation of *Jewel* to *Hepting* or assignment of *Jewel* to the MDL. He further indicated to Ms. Cohn that based on a voicemail message he had received from AT&T counsel Bradford Berenson, he believed that AT&T would oppose, although he noted that the voicemail was somewhat garbled.

2. To seek clarity on the Government and AT&T's position on the matter, on Friday, October 3, 2008, I circulated via email to Mr. Coppolino and Mr. Berenson a copy of our draft motion to relate the cases, seeking their consent and requesting a response by Wednesday, October 8, 2008.

3. Mr. Berenson responded to me by email on Monday, October 6, 2008, stating in relevant part that:

AT&T has reviewed your draft and decided that it will not oppose the motion. AT&T does not wish to join in the motion or to be represented as affirmatively consenting or stipulating, but you may represent that AT&T has no objection to the requested relief and does not oppose the motion. It is possible that after you file, AT&T may make a very short submission explaining its non-opposition.

4. After alerting me in a timely manner that there would be a slight delay in his response as he consulted with his clients, Mr. Coppolino responded to me by email on Thursday, October 9, 2008, stating in relevant part that:

The Government Defendants sued in their official capacity in the *Jewel* case (08-cv-4373-CRB) do not oppose the relief requested in your administrative motion, made pursuant to Local Rule 3-12, for an Order relating *Jewel* to the *Hepting* case (06-cv-00672-VRW) and, in turn, for the assignment of *Jewel* to MDL 06-cv-1791-VRW pursuant to MDL Rule 7.5(a). Other than this consent, the Government Defendants do not agree to or adopt any statement or representation made in the motion itself.

5. Mr. Coppolino further explained in a subsequent email on October 9 that the appropriate contact regarding the personal capacity Defendants in *Jewel* was trial attorney Jim Whitman of the Constitutional Torts Section of the Torts Branch of the U.S. Department of

1 Justice's Civil Division. I emailed the draft motion to Mr. Whitman, along with our draft proposed
2 order, that same day, seeking his consent on behalf of the Jewel personal capacity Defendants.

3 6. The next day, Friday, October 10, 2008, Mr. Whitman left a voicemail message for
4 me indicating that because he had not yet secured authority to represent all of the individual
5 personal capacity Defendants in Jewel, and because those Defendants had not yet been served with
6 the Jewel complaint, he was unable to provide—and did not believe Plaintiffs required—the
7 consent of those Plaintiffs.

8 7. Mr. Whitman summarized his voicemail in an email to me later that same day. In
9 relevant part:

10 To summarize, I do not yet have authority to represent all the individual Defendants
11 in their personal capacity. With that, and because those Defendants have not yet
12 been served in their personal capacity (for the same reason, I'm still working on
13 getting authority to accept service on behalf of the Defendants), I am not in a
14 position to oppose or not oppose Plaintiffs' motion to relate. In theory, I see no
15 reason to oppose that motion, but I simply cannot make that representation at this
16 time. So, since the individual Defendants are technically not "in the case" yet, I see
17 no problem with Plaintiffs going forward with their motion to relate without
18 obtaining the individual Defendants' consent (or, more accurately, non-opposition).

19 8. On Tuesday, October 14, 2008, I was informed by Plaintiffs' counsel and EFF Civil
20 Liberties Director Jennifer Granick, who had been conferring with Mr. Whitman on service issues,
21 that he had indicated to her by phone that afternoon that he had secured authority to represent the
22 individual Jewel Defendants in their personal capacity and that he could accept service of
23 Plaintiffs' motion to relate Jewel to Hepting, but again indicating that he could not and need not
24 consent to such because the individual Defendants had not yet been served with the complaint.

25 9. Ms. Granick forwarded to me on October 14, 2008 an email from Mr. Whitman sent
26 to her that same day summarizing their discussion, which stated in relevant part:

27 As I indicated, I am now authorized to represent all of the individual Defendants in
28 the *Jewel* case in their individual capacities.... [T]his [email] will confirm that I am
authorized to accept service of Plaintiffs' motion to relate the case and motion to
reassign it to the MDL on behalf of the individual Defendants. For that purpose,
you can serve me ... by e-mail at this e-mail address.

1 I declare under penalty of perjury under the laws of the United States of America that the
2 foregoing is true and correct.

3
4 DATED: October 21, 2008

5 By /s/ Kevin S. Bankston
6 KEVIN S. BANKSTON
7 454 Shotwell Street
8 San Francisco, CA 94110
9 Telephone: 415/436-9333
10 415/436-9993 (fax)

PROOF OF SERVICE

I am a citizen of the United States and employed in San Francisco County, California. I am over the age of eighteen years and not a party to the within-entitled actions. My business address is 454 Shotwell Street, San Francisco, California 94110. On October 21, 2008, I served true and correct copies of the documents described as

- ADMINISTRATIVE MOTION BY PLAINTIFFS TO CONSIDER WHETHER CASES SHOULD BE RELATED; SUPPORTING DECLARATION OF KEVIN S. BANKSTON; and
- PROPOSED ORDER DEEMING CASES RELATED AND ASSIGNING *JEWEL* TO MDL Docket No 06-1791 VRW, IN RE NATIONAL SECURITY AGENCY TELECOMMUNICATIONS RECORDS LITIGATION

BY EMAIL on JAMES WHITMAN, trial attorney, U.S. Department of Justice, Civil Division, Torts Branch, Constitutional Torts Section, counsel to the personal capacity Defendants in *Jewel, et al., v. NSA, et al.*, No. C-08-4373-CRB, by transmitting copies of the documents to James.Whitman@usdoj.gov, and

BY ELECTRONIC FILING using the Court's CM/ECF system on the parties to *Hepting, et al. v. AT&T Corp. et al.*, No. C-06-0672-VRW, counsel for whom includes counsel for the government Defendants in *Jewel*.

I declare that I am a member of the bar of this court at whose direction the service was made.

Executed on October 21, 2008, at San Francisco, California.

/s/ Kevin S. Bankston
KEVIN S. BANKSTON

1 Ilann M. Maazel (*pro hac vice*)
Matthew D. Brinckerhoff (*pro hac vice*)
2 Adam R. Pulver (SBN # 268370)
EMERY CELLI BRINCKERHOFF & ABADY LLP
3 75 Rockefeller Plaza, 20th Floor
New York, New York 10019
4 Telephone: (212) 763-5000
Facsimile: (212) 763-5001
5 Attorneys for Plaintiffs

6
7 **IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF CALIFORNIA**

8 IN RE NATIONAL SECURITY AGENCY)
TELECOMMUNICATIONS RECORDS)
9 LITIGATION)

Case No. 3:06-md-1791-VRW

10 This Document Relates to:

**SECOND AMENDED CLASS
ACTION COMPLAINT/
DEMAND FOR JURY TRIAL**

11 VIRGINIA SHUBERT, NOHA ARAFA,
SARAH DRANOFF and HILARY
12 BOTEIN, individually and on behalf of all
others similarly situated,

13 Plaintiffs,

14 -against -

15 BARACK OBAMA, KEITH B. .
16 ALEXANDER, ERIC HOLDER,
MICHAEL HAYDEN, ALBERTO
17 GONZALES, JOHN ASHCROFT,
UNITED STATES OF AMERICA, and
18 JOHN/JANE DOES #1-100 (07-693)

19 Plaintiffs Virginia Shubert, Noha Arafa, Sarah Dranoff, and Hilary Botein, by their
20 attorneys Emery Celli Brinckerhoff & Abady LLP, for their Second Amended Complaint, allege as
21 follows:
22
23
24
25
26
27
28

PRELIMINARY STATEMENT

1
2 1. This class action challenges a secret government spying program pursuant
3 to which, on information and belief, virtually every telephone, Internet and email communication
4 sent from or received within the United States since shortly after September 11, 2001 has been (and
5 continues to be) searched, seized, intercepted, and subjected to surveillance without a warrant,
6 court order or any other lawful authorization in violation of the Foreign Intelligence Surveillance
7 Act of 1979, 50 U.S.C. § 1810.

8 2. Without the approval of Congress, without the approval of any court, and
9 without notice to the American people, President George W. Bush authorized a secret program to
10 spy upon millions of innocent Americans, including the named plaintiffs. As one former NSA
11 employee admitted, "The National Security Agency had access to *all* Americans' communications:
12 faxes, phone calls, and their computer communications . . . It didn't matter whether you were in
13 Kansas, you know, in the middle of the country and you never made foreign communications at all.
14 They monitored all communications."¹ This program (the "Spying Program") – intercepting,
15 searching, seizing, and subjecting to surveillance the content of personal phone conversations,
16 email, and Internet searches of millions of unsuspecting, innocent Americans – is illegal. It
17 violates the plain terms of federal statutes that make such conduct a crime.² It violates the most
18 basic principles of separation of powers. It violates the Constitution.

19 3. The government's spy agency, the National Security Agency ("NSA"), spied
20 upon Americans at home. It spied upon Americans at work. And it is spying today, and will
21 continue to spy on millions of innocent, unsuspecting Americans, unless stopped by a federal court.

22 4. The existence and operation of this secret spying program has been
23 acknowledged by numerous executive officials, including former President Bush in December
24
25

26 ¹ <http://www.youtube.com/watch?v=osFprWnCjPA> at 2:15 (statement by NSA operative Russell
Tice).

27 ² *E.g.* The Foreign Intelligence Surveillance Act, 50 U.S.C. § 1801 *et seq.* ("FISA"); the Wiretap
28 Act 18 U.S.C. § 2510 *et seq.*; the Stored Communications Act, 18 U.S.C. § 2701 *et seq.* ("SCA").

1 2005, former Attorney General Alberto Gonzales and former Director of National Intelligence
2 Michael Hayden, as well as high-level officials in the NSA.

3 5. As part of the Spying Program, defendants have not only eavesdropped on
4 specific communications by American citizens, they have also intercepted and continue to intercept
5 *en masse* the communications of millions of ordinary Americans – estimated at between 15 and 20
6 *trillion* communications over the past eleven years.

7 6. Defendants have achieved this dragnet in part by attaching sophisticated
8 communications surveillance devices to the key facilities of numerous telecommunications
9 companies, including AT&T and Verizon (used by the named plaintiffs), that transmit and receive
10 Americans' Internet and telephone communications.

11 7. Using these surveillance devices, defendants have acquired and continue to
12 acquire the content of phone calls, emails, instant messages, text messages, web communications
13 and other communications, both international and domestic, of millions of Americans who use the
14 phone system or the Internet, including Plaintiffs and class members.

15 8. Having unlawfully acquired and intercepted millions of communications
16 from United States persons, the NSA searches for keywords, phrases, or names it deems suspicious,
17 in order to select which communications are subjected to yet further analysis by staff of the NSA,
18 as part of a vast data-mining operation.

19 9. The American people deserve better. The American people should not be
20 subjected to a illegal, covert, dragnet spying operation by their own government. This class action
21 is brought on behalf of all present and future United States persons who have been or will be
22 subject to electronic surveillance by the National Security Agency without a search warrant, court
23 order, or other lawful authorization since September 12, 2001.³ It primarily seeks liquidated
24 damages under the Federal Intelligence Surveillance Act 50 U.S.C. § 1810 *et. seq.* ("FISA"), which
25 authorizes civil actions for violations of FISA.

26
27 ³ "United States persons" and "electronic surveillance" are both defined terms set forth in FISA.
28 50 U.S.C. § 1801.

PARTIES.

10. Plaintiff Virginia Shubert is an American citizen who resides and works in Brooklyn, New York. Ms. Shubert regularly makes phone calls and sends email both within the United States, and outside the United States. Ms. Shubert, for example, frequently calls and sends emails to the United Kingdom, France and Italy and has made similar communications as a part of her work. Since September 12, 2001, Ms. Shubert has been and continues to be a customer of AT&T, which participated and participates in the Spying Program. Pursuant to the illegal Spying Program, Ms. Shubert's phone calls and emails have repeatedly been surveilled and intercepted by the NSA without a warrant or other judicial authorization. On information and belief, Ms. Shubert's illegally intercepted communications are currently in the custody, control, and possession of the NSA.

11. Plaintiff Noha Arafa is an American citizen who resides and works in Brooklyn, New York. She regularly makes phone calls and sends email both within the United States, and outside the United States. Ms. Arafa, for example, frequently calls and sends emails to family and friends in Egypt from her home, and has made telephone calls abroad as a part of her work. Since September 12, 2001, Ms. Dranoff has been and continues to be a customer of a customer of AT&T, which participated and participates in the Spying Program. Pursuant to the illegal Spying Program, Ms. Arafa's phone calls and emails have repeatedly been surveilled and intercepted by the NSA without a warrant or other judicial authorization. On information and belief, Ms. Arafa's illegally intercepted communications are currently in the custody, control, and possession of the NSA.

12. Plaintiff Sarah Dranoff is an American citizen who resides and works in Brooklyn, New York. Ms. Dranoff regularly makes phone calls and sends email both within the United States, and outside the United States. Ms. Dranoff for example, calls the Netherlands and sends emails to the Netherlands and Norway from her home. Since September 12, 2001, Ms. Dranoff has been a customer of Verizon and of AT&T, which, on information and belief, participated and participates in the Spying Program. Pursuant to the illegal Spying Program, Ms. Dranoff's phone calls and emails have repeatedly been surveilled and intercepted by the NSA

1 without a warrant or other judicial authorization. On information and belief, Ms. Dranoff's
2 illegally intercepted communications are currently in the custody, control, and possession of the
3 NSA.

4 13. Plaintiff Hilary Botein is an American citizen who resides and works in
5 Brooklyn, New York. Ms. Botein makes phone calls and sends email both within the United
6 States, and outside the United States. Since September 12, 2001, Ms. Botein has been a customer
7 of Verizon which, on information and belief, participated and participates in the Spying Program.
8 Pursuant to the illegal Spying Program, Ms. Botein's phone calls and emails have repeatedly been
9 surveilled and intercepted by the NSA without a warrant or other judicial authorization. On
10 information and belief, Ms. Botein's illegally intercepted communications are currently in the
11 custody, control, and possession of the NSA.

12 14. Defendant Barack H. Obama is the President of the United States, and sued
13 solely in his official capacity. Mr. Obama's predecessor, George W. Bush, authorized the illegal
14 Spying Program, and Mr. Obama has continued and continues to authorize the illegal Spying
15 Program.

16 15. Defendant Lieutenant General Keith B. Alexander is the Director of the
17 NSA, and is sued in both his personal and official capacities. Since 2005, Defendant Alexander
18 has had ultimate authority for supervising and implementing all operations and functions of the
19 NSA, including the illegal Spying Program.

20 16. Defendant Eric Holder is the Attorney General of the United States, and is
21 sued solely in his official capacity. On information and belief, Mr. Holder approved and authorized
22 the Spying Program. Mr. Holder's predecessor, Defendant Gonzales approved and authorized the
23 Spying Program and has consistently defended the program before Congress and in other public
24 fora.

25 17. Defendant Lieutenant General Michael V. Hayden is the former Director of
26 the NSA, and is sued solely in his personal capacity. While Director, defendant Hayden had
27 ultimate authority for supervising and implementing all operations and functions of the NSA,
28

1 including the illegal Spying Program.. Defendant Hayden also apparently approved the illegal
2 initiation of the Spying Program.

3 18. Defendant Alberto Gonzales is the former Attorney General of the United
4 States. Defendant Gonzales approved and authorized the Spying Program and has consistently
5 defended the program before Congress and in other public fora.

6 19. Defendant John Ashcroft is the former Attorney General of the United States.
7 Although, according to some published reports, defendant Ashcroft had reservations concerning the
8 Spying Program, Mr. Ashcroft ultimately approved and authorized the Spying Program.

9 20. Each of the individual defendants works or worked for the government of the
10 United States of America, which has conducted and continues to conduct the illegal Spying
11 Program.

12 21. At all times relevant hereto, defendants John and Jane Does #1-100 (the
13 "Doe defendants"), whose actual names plaintiff has been unable to ascertain notwithstanding
14 reasonable efforts to do so, but who are sued herein by the fictitious designation "John Doe" and
15 "Jane Doe," were agents and employees of the NSA, Department of Homeland Security,
16 Department of Justice, the White House, or other government agencies, acting in the capacity of
17 agents, servants, and employees of the United States government, and within the scope of their
18 employment as such, who conducted, authorized, and/or participated in the Spying Program.

19
20 **JURISDICTION AND VENUE**

21 22. This action arises under the Fourth Amendment to the United States
22 Constitution, the Foreign Intelligence Surveillance Act, 50 U.S.C. § 1801 *et seq.*, the Wiretap Act
23 18 U.S.C. § 2510 *et seq.*; and the Stored Communications Act, 18 U.S.C. § 2701 *et seq.*

24 23. The jurisdiction of this Court is predicated upon 28 U.S.C. §§ 1331,
25 1343(a)(4).

26 24. Venue is proper in this transferee district pursuant to an Order of the Judicial
27 Panel on Multi-District Litigation, pursuant to 28 U.S.C. § 1407, and is proper in the transferor
28 district (Eastern District of New York), pursuant to 28 U.S.C. § 1391(e).

JURY DEMAND

25. Plaintiffs demand trial by jury in this action.

CLASS ACTION ALLEGATIONS

26. The plaintiff class seeks (i) a judgment declaring that the Spying Program violates FISA, the Wiretap Act, the SCA, and the Fourth Amendment; (ii) an order enjoining defendants from continuing the Spying Program or otherwise subjecting United States persons to electronic surveillance by the NSA without a search warrant or court order; (iii) an order requiring defendants to delete and destroy, permanently and irrevocably, every communication and record of every communication intercepted by the NSA pursuant to the Spying Program in the custody, control, or possession of the United States or any of its agents or employees; and (iv) liquidated damages as set forth in 50 U.S.C. § 1810, and 18 U.S.C. §§ 2520, 2707 to redress the extraordinary invasion of privacy caused by the Spying Program.

27. Plaintiffs sue on behalf of themselves and all other similarly situated individuals, and seek to represent a class comprised of all present and future United States persons who have been or will be subject to electronic surveillance by the National Security Agency without a search warrant, court order, or other lawful authorization since September 12, 2001.

28. The members of the class are so numerous as to render joinder impracticable.

29. The questions of law and fact common to the class include that the class members were all subject to electronic surveillance without a search warrant, court order, or any lawful authorization pursuant to the Spying Program; all have the common right under FISA, the Wiretap Act, and the SCA to be free from electronic surveillance absent a search warrant or court order, the common right under FISA, the Wiretap Act, and the SCA to liquidated damages for violations of those rights, and the common right under the Fourth Amendment to be free from electronic surveillance absent a search warrant or court order. Defendants' electronic surveillance without a search warrant, court order, or any lawful authorization violated those rights.

1 30. The named plaintiffs are adequate representatives of the class. The
2 violations of law alleged by the named plaintiffs stem from the same course of conduct by
3 defendants – failure to seek a search warrant, court order, or any other lawful authorization before
4 conducting electronic surveillance – that violated and continue to violate the rights of members of
5 the class; the legal theory under which the named plaintiffs seek relief is the same or similar to that
6 on which the class will rely. In addition, the harms suffered by the named plaintiffs are typical of
7 the harms suffered by the class members, especially given the common calculation of liquidated
8 damages.

9 31. The named plaintiffs have the requisite personal interest in the outcome of
10 this action and will fairly and adequately protect the interests of the class. The named plaintiffs are
11 represented by Emery Celli Brinckerhoff & Abady LLP (“ECBA”). Counsel has the resources,
12 expertise and experience to prosecute this action. Counsel for the plaintiffs knows of no conflicts
13 among members of the class or between ECBA and members of the class.

14 32. A class action is superior to other available methods for the fair and efficient
15 adjudication of this controversy because: (i) the prosecution of millions of separate actions would
16 be inefficient and wasteful of legal resources; (ii) the members of the class are scattered throughout
17 the United States and are not likely to be able to vindicate and enforce their statutory and
18 constitutional rights unless this action is maintained as a class action; (iii) the issues raised can be
19 more fairly and efficiently resolved in the context of a single class action than piecemeal in many
20 separate actions; (iv) the resolution of litigation in a single forum will avoid the danger and
21 resultant confusion of possible inconsistent determinations; (v) the prosecution of separate actions
22 would create the risk of inconsistent or varying adjudications with respect to individuals pursuing
23 claims against defendants which would establish incompatible standards of conduct for defendants;
24 and (vi) questions of law and/or fact common to members of the class predominate over any
25 question that affects individual members.

26
27
28

FACTUAL ALLEGATIONS

Classwide Allegations

Legal Framework

33. The Fourth Amendment provides that “[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.”

34. Congress has enacted two statutes that together supply “the *exclusive means* by which electronic surveillance . . . and the interception of domestic wire, oral, and electronic communications may be conducted.” 18 U.S.C. § 2511(2)(f) (emphasis added). The first is the Electronic Communications Privacy Act (“ECPA”), which includes the Wiretap Act, 18 U.S.C. § 2510 *et seq.*, and the Stored Communications Act, 18 U.S.C. § 2701 *et seq.*, and the second is the Foreign Intelligence Surveillance Act, 50 U.S.C. § 1801 *et seq.* (“FISA”).

The ECPA

35. Congress first enacted the predecessor to the ECPA (commonly referred to as Title III) in response to the U.S. Supreme Court’s recognition, in *Katz v. United States*, 389 U.S. 347 (1967), that individuals have a constitutionally protected privacy interest in the content of their telephone calls. Through Title III and then the ECPA, Congress created a statutory framework to govern the surveillance of wire and oral communications in law enforcement investigations.

36. The ECPA authorizes the government to intercept wire, oral, or electronic communications in investigations of certain enumerated criminal offenses, *see* 18 U.S.C. § 2516, with prior judicial approval, *see id.* § 2518.

37. In order to obtain a court order authorizing the interception of a wire, oral, or electronic communication, the government must demonstrate that “there is probable cause for belief that an individual is committing, has committed, or is about to commit” one of the enumerated criminal offenses. *Id.* § 2518(3)(a).

1 38. It must also demonstrate, among other things, that “there is probable cause
2 for belief that particular communications concerning [the enumerated] offense will be obtained
3 through [the] interception,” *id.* § 2518(3)(b), and that “normal investigative procedures have been
4 tried and have failed or reasonably appear to be unlikely to succeed if tried or to be too dangerous,”
5 *id.* § 2518(3)(c).

6 39. The ECPA specifies civil and criminal penalties for surveillance that is not
7 authorized. *See id.* §§ 2511, 2520, 2701, 2707.

8
9 **Foreign Intelligence Surveillance Act**

10 40. The government has one and only one other legal avenue to engage in
11 electronic surveillance: the Foreign Intelligence Surveillance Act.

12 41. In 1978, Congress enacted FISA to govern the use of electronic surveillance
13 against foreign powers and their agents inside the United States. The statute created the Foreign
14 Intelligence Surveillance Court, a court composed of seven (now eleven) federal district court
15 judges, and empowered this court to grant or deny government applications for electronic
16 surveillance orders in foreign intelligence investigations. *See* 50 U.S.C. § 1803(a). Congress
17 enacted FISA after the U.S. Supreme Court held, in *United States v. United States District Court*
18 *for the Eastern District of Michigan*, 407 U.S. 297 (1972), that the Fourth Amendment does not
19 permit warrantless surveillance in intelligence investigations of domestic security threats. FISA
20 was a response to that decision and to the Report of the Senate Select Committee to Study
21 Government Operations with Respect to Intelligence Activities, S.Rep. No. 94-755, 94th Cong., 2d
22 Sess. (1976) (“Church Committee Report”), which found that the executive had engaged in
23 warrantless wiretapping of numerous United States citizens – including journalists, activists, and
24 Congressmen – who posed no threat to the nation’s security and who were not suspected of any
25 criminal offense. The Church Committee Report warned that “[u]nless new and tighter controls are
26 established by legislation, domestic intelligence activities threaten to undermine our democratic
27 society and fundamentally alter its nature.”

1 42. When Congress enacted FISA, it provided that the procedures set out therein
2 “shall be the *exclusive means* by which electronic surveillance . . . and the interception of domestic
3 wire, oral, and electronic communications may be conducted.” 18 U.S.C. § 2511(2)(f) (emphasis
4 added).

5 43. FISA provides that no one may engage in electronic surveillance “except as
6 authorized by statute,” *id.* § 1809(a)(1).

7 44. FISA specifies civil and criminal penalties for electronic surveillance
8 undertaken without statutory authority, *see id.* §§ 1809 & 1810.

9 45. The Senate Judiciary Committee explained that “[t]he basis for this
10 legislation is the understanding – concurred in by the Attorney General – that even if the President
11 has an ‘inherent’ Constitutional power to authorize warrantless surveillance for foreign intelligence
12 purposes, Congress has the power to regulate the exercise of this authority by legislating a
13 reasonable warrant procedure governing foreign intelligence surveillance.” S. Rep. 95-604(I),
14 reprinted at 1978 U.S.C.C.A.N. at 3917. The Committee further explained that the legislation was
15 meant to “spell out that the executive cannot engage in electronic surveillance within the United
16 States without a prior Judicial warrant.” *Id.* at 3906.

17 46. FISA defines “electronic surveillance” to include:

18 a. “the acquisition by an electronic, mechanical, or other
19 surveillance device of the contents of any wire or radio
20 communication sent by or intended to be received by a
21 particular, known United States person who is in the United
22 States, if the contents are acquired by intentionally targeting
23 that United States person, under circumstances in which a
24 person has a reasonable expectation of privacy and a warrant
25 would be required for law enforcement purposes”;

26
27 b. “the acquisition by an electronic, mechanical, or other
28 surveillance device of the contents of any wire

1 communication to or from a person in the United States, . . .
2 without the consent of any party thereto, if such acquisition
3 occurs in the United States . . .”;

4
5 c. “the intentional acquisition by an electronic, mechanical, or
6 other surveillance device of the contents of any radio
7 communication, under circumstances in which a person has a
8 reasonable expectation of privacy and a warrant would be
9 required for law enforcement purposes, and if both the sender
10 and all intended recipients are located within the United
11 States”; and

12
13 d. “the installation or use of an electronic, mechanical, or other
14 surveillance device in the United States for monitoring to
15 acquire information, other than from a wire or radio
16 communication, under circumstances in which a person has a
17 reasonable expectation of privacy and a warrant would be
18 required for law enforcement purposes.” 50 U.S.C. § 1801(f).

19
20 47. FISA defines “contents” to include “any information concerning the identity
21 of the parties to such communication or the existence, substance, purport, or meaning of that
22 communication.” 50 U.S.C. § 1801(n).

23 48. FISA defines “United States person” to include United States citizens and
24 lawful permanent residents. *Id.* § 1801(d).

25 49. In order to obtain an order from the FISA Court authorizing electronic
26 surveillance, the government must demonstrate, among other things, probable cause to believe that
27 “the target of the electronic surveillance is a foreign power or an agent of a foreign power” and that
28

1 “each of the facilities or places at which the electronic surveillance is directed is being used, or is
2 about to be used, by a foreign power or an agent of a foreign power.” *Id.* § 1805(a)(3).

3 50. While FISA generally prohibits surveillance without prior judicial
4 authorization, it includes a provision that allows for warrantless surveillance in “emergency
5 situation[s].” Where an emergency situation exists and “the factual basis for issuance of an order
6 under this subchapter to approve such surveillance exists,” the statute permits the Attorney General
7 to authorize warrantless surveillance “if a judge having jurisdiction under section 1803 of this title
8 is informed by the Attorney General or his designee at the time of such authorization that the
9 decision has been made to employ emergency electronic surveillance and if an application in
10 accordance with this subchapter is made to that judge as soon as practicable, but not more than 72
11 hours after the Attorney General authorizes such surveillance.” *Id.* § 1805(f).

12 51. FISA also permits electronic surveillance without a court order for fifteen
13 days after a formal declaration of war. *Id.* § 1811 (“Notwithstanding any other law, the President,
14 through the Attorney General, may authorize electronic surveillance without a court order under
15 this subchapter to acquire foreign intelligence information for a period not to exceed fifteen
16 calendar days following a declaration of war by the Congress.”).

17 52. FISA requires the Attorney General to report to the House and Senate
18 Intelligence Committees twice a year regarding “all electronic surveillance” authorized under
19 FISA. *Id.* § 1808(a). Statistics released annually by the Justice Department indicate that, between
20 1978 and 2004, the government submitted almost 19,000 surveillance applications to the FISA
21 Court. The FISC denied four of these applications; granted approximately 180 applications with
22 modifications; and granted the remainder without modifications.

23 **The Creation of the Spying Program**

24 53. Until December 2005, even the existence of the Spying Program was
25 unknown to Congress and to the American people.

26 54. To the contrary, in a speech on June 9, 2005, President Bush stated: “*Law*
27 *enforcement officers need a federal judge’s permission to wiretap a foreign terrorist’s phone, a*
28 *federal judge’s permission to track his calls, or a federal judge’s permission to search his property.*”

1 *Officers must meet strict standards to use any of these tools. And these standards are fully*
2 consistent with the Constitution of the U.S.” (Emphasis supplied.)⁴

3 55. Although it is true that federal law requires law enforcement officers to get
4 permission from a federal judge to wiretap, track, or search, President Bush secretly authorized a
5 Spying Program that did none of those things.

6 56. As revealed in *The New York Times* in December 2005, and as subsequently
7 revealed by, *inter alia*, published press reports, whistleblowers, insiders within the United States
8 government, top government officials, and (after initial equivocation) President Bush himself, in
9 the fall of 2001 the NSA launched a secret electronic surveillance program to intercept, search and
10 seize, without prior judicial authorization, the telephone and Internet communications of people
11 inside the United States. This program, as Rep. Silvestre Reyes, then-Chairman of the House
12 Permanent Select Committee On Intelligence (who has been briefed on the Program), explained at
13 a September 2007 hearing, “involved not only targets overseas, but also American citizens whose
14 phone calls were listened to and e-mail read without a warrant.”

15 57. On or around October 4, 2001, President Bush issued an order authorizing
16 the NSA to conduct surveillance of telephone and Internet communications of persons within the
17 United States, without court-approved warrants or other judicial authorization. The Spying
18 Program began on or around October 6, 2001. While President Bush ultimately signed the
19 Program Order initiating the Program, Vice President Cheney and the legal counsel to the Office of
20 the Vice President, David Addington, “guided the program’s expansion and development.”
21 According to one former DOJ Official, Addington was the “chief legal architect” of the Program,
22 and he and Cheney “had abhorred FISA’s intrusion on presidential power ever since its enactment
23 in 1978. After 9/11 they and other top officials in the administration dealt with FISA the way they
24 dealt with other laws they didn’t like: They blew through them in secret based on flimsy legal
25 opinions that they guarded closely so no one could question the legal basis for the operations.”

26
27
28 ⁴ See <http://georgewbush-whitehouse.archives.gov/news/releases/2005/06/20050609-2.html>.

1 58. . . . President Bush reauthorized the Spying Program more than 30 times
2 between October 2001 and December 2006, approximately every 45 days, as confirmed by
3 responses by the Office of the Vice President to a Congressional subpoena.

4 59. The Program reflects a goal of the NSA presented to the incoming Bush
5 administration in December 2000. A transition document for the new administration stated "The
6 volumes and routing of data make finding and processing nuggets of intelligence information more
7 difficult. To perform both its offensive and defensive mission, NSA must 'live on the network.'"
8 Moreover, the NSA asserted that its "mission will demand a powerful, permanent presence on a
9 global telecommunications network that will host the 'protected' communications of Americans as
10 well as the targeted communications of adversaries."

11 60. Addington and then-White House Counsel Alberto Gonzales assigned John
12 Yoo, then a Deputy Assistant Attorney General in the Office of Legal Counsel, to prepare legal
13 opinions in support of the Program. The Department of Justice prepared memoranda dated October
14 4 and November 2, 2001; January 9, May 17, and October 11, 2002; February 25, 2003; March 15,
15 May 6, and July 16, 2004; and February 4, 2005. Years later, after he left government service in
16 2003, Yoo explained why FISA was not sufficient for the Program's dragnet interception:

17 [U]nder existing laws like FISA, you have to have the name of somebody,
18 have to already suspect that someone's a terrorist before you can get a
19 warrant. You have to have a name to put in the warrant to tap their phone
20 calls, and so it doesn't allow you as a government to use judgment based on
21 probability to say: "Well, 1 percent probability of the calls from or maybe 50
22 percent of the calls are coming out of this one city in Afghanistan, and
23 there's a high probability that some of those calls are terrorist
24 communications. But we don't know the names of the people making those
25 calls." You want to get at those phone calls, those e-mails, but under FISA
26 you can't do that.

27
28

1 61. The government has candidly admitted that FISA “requires a court order
2 before engaging in this kind of surveillance . . . unless otherwise authorized by statute or by
3 Congress.” The Program admittedly operates “in lieu of” court orders or other judicial
4 authorization, and neither the President nor Attorney General authorizes the specific interceptions.
5 As General (Ret.) Michael V. Hayden, the former Principal Deputy Director for National
6 Intelligence, put it, the Program “is a more . . . ‘aggressive’ program than would be traditionally
7 available under FISA,” in part because “[t]he trigger is quicker and a bit softer than it is for a FISA
8 warrant.” The only review process is authorization by an NSA “shift supervisor” for direct review
9 of particular individuals’ communication.

10 **The Mechanics of the Spying Program**

11 62. As part of the Spying Program, the NSA uses satellite dishes controlled both
12 by the NSA and those controlled by telecommunications companies to intercept, search and seize,
13 and subject to electronic surveillance communications that are transmitted via satellite. Many of
14 these satellite dishes are located within the United States.

15 63. According to the Senate Select Committee on Intelligence, shortly after
16 September 11, 2011, the Executive branch sent letters requesting or directing U.S. electronic
17 communication service providers to provide access to communications in order to assist the NSA
18 with intelligence activities that had been authorized by the President. In a Report, the Committee
19 confirmed: “The letters were provided to electronic communication service providers at regular
20 intervals. All of the letters stated that the activities had been authorized by the President. All of the
21 letters also stated that the activities had been determined to be lawful by the Attorney General,
22 except for one letter that covered a period of less than sixty days. That letter, which like all the
23 others stated that the activities had been authorized by the President, stated that the activities had
24 been determined to be lawful by the Counsel to the President.”

25 64. The “assistance” sought involved an important aspect of the Spying Program
26 challenged here. The NSA uses electronic communication companies, including AT&T and
27 Verizon (used by the named plaintiffs), to intercept, search and seize, and subject to electronic
28 surveillance communications, including voice calls and e-mails, that pass through switches

1 controlled by these companies. These switches are the hubs through which voice calls and data.
2 transmissions are routed every second.

3 65. These switches, which are located inside the United States, serve as primary
4 gateways for communications going into, through, and out of the United States. The switches
5 connect to transoceanic fiber-optic cables that transmit communications to other countries.

6 66. In January 2006, a former AT&T employee named Mark Klein provided
7 detailed eyewitness testimony and documentary evidence showing how telecommunications
8 companies in general, and AT&T in particular, are acquiring communications for the government.
9 Klein had worked as an AT&T technician for 22 years, most recently at AT&T's San Francisco
10 facility on Folsom Street.

11 67. The NSA has worked with telecommunications and Internet providers in the
12 United States to install "splitters" on fiber-optic cables carrying domestic and international
13 communications. According to William Binney, the former chief and co-founder of the NSA's
14 Signals Intelligence Automation Research Center, and a former senior NSA crypto-mathematician,
15 there are between 10 and 20 such splitters installed throughout the country—"not just San
16 Francisco; they have them in the middle of the country and also on the East Coast."⁵ The
17 installation of these splitters allows two identical copies of all communications to be made, with
18 one copy traveling its intended course, and the other being routed to the NSA. These
19 communications are routed *en masse* to the NSA without any concern for the subject matter or
20 content of the communications.

21 68. Former AT&T employee Klein has provided documents showing how these
22 splitters operate, and divert communications to the NSA, at one AT&T facility. To divert the
23 communications, AT&T connected the fiber-optic cables entering its WorldNet Internet room to a
24 "splitter cabinet." The splitter cabinet splits the light signals from the WorldNet Internet service in
25 two, making two identical copies of the material carried on the light signal. The splitter cabinet

26 ⁵ James Bamford, "The NSA is Building the Country's Biggest Spy Center (Watch What You
27 Say)," *Wired Threat Level* Blog (Mar. 15, 2012), [http://www.wired.com/threatlevel/](http://www.wired.com/threatlevel/2012/03/ff_nsadatacenter/)
28 2012/03/ff_nsadatacenter/; also available as James Bamford, "Inside the Matrix," *Wired*, April
2012, at 78.

1 directs one portion of the light signal through fiber optic cables into a secret room built on AT&T
2 premises, but controlled by the NSA while allowing the other portion to travel its normal course to
3 its intended destination. The split cables carry domestic and international communications of
4 AT&T customers, as well as communications from users of other non-AT&T networks that pass
5 through that facility. The position or location of the fiber split make clear that it was not designed
6 to capture only international traffic, and necessarily captures purely domestic communications, as a
7 fiber splitter is not a selective device. According to Klein, AT&T intercepts every single one of the
8 communications passing through the WorldNet Internet room and directs them all to the NSA.
9 Klein and others have reported similar splitters throughout the United States. Klein's report has
10 been confirmed by James Russell, AT&T's Managing Director-Asset Protection.

11 69. According to former NSA official Binney, at the outset of this program, the
12 NSA recorded 320 million calls a day – a number that has since increased.⁶

13 70. After the communications are acquired by the NSA, they are subjected to an
14 initial computer-controlled analysis to "listen" to the content of the communications, search for
15 targeted addresses, locations, countries, phone numbers, keywords, phrases, and watch-listed
16 names, and analyze patterns, referred to by former Secretary of Homeland Security Michael
17 Chertoff as "data-mining." This analysis intrudes into content, and the computers "listen" to more
18 Americans than humans do. The Program uses extremely powerful computerized search
19 programs—originally intended to scan foreign communications—to scrutinize large volumes of
20 American communications. According to a recent article based on interviews with former NSA
21 officials, "Any communication that arouses suspicion, especially to or from the million or so
22 people on agency watch lists, are automatically copied or recorded,"⁷ and subjected to human
23 review. Once an individual has been "flagged," all calls and communications to or from that
24 individual are automatically routed to the NSA's recorders.

25 71. Government officials have acknowledged that "most telephone calls in the
26 United States" are subjected to such searches, regardless of whether there was any suspicion of the

27 ⁶ *Id.*

28 ⁷ *Id.*

1 sender or recipient.. As one official explained, "you have to have all the calls or most of them. But
2 you wouldn't be interested in the vast majority of them."

3 72. One way communications are searched is by keywords. If the keywords
4 included "jihad," "Iraq," "Bush is a criminal," or whatever words or phrases the United States
5 government deems of interest, then, pursuant to the Spying Program, the Americans who use such
6 terms may be targeted by the NSA for even further interception, search and seizure, and electronic
7 surveillance.

8 73. As reported in *The Wall Street Journal*, the data-sifting effort can also begin
9 by using a phone number or web address as a lead. "In partnership with the FBI, the systems then
10 can track all domestic and foreign transactions of people associated with that item -- and then the
11 people who associated with them, and so on, casting a gradually wider net. An intelligence official
12 described more of a rapid-response effect: If a person suspected of terrorist connections is believed
13 to be in a U.S. city -- for instance, Detroit, a community with a high concentration of Muslim
14 Americans -- the government's spy systems may be directed to collect and analyze all electronic
15 communications into and out of the city."

16 74. NSA employees have also confirmed that they have personally listened in on
17 hundreds of citizens' phone calls that have no connection to national security, including calls
18 between Americans and their family members abroad and calls regarding international aid
19 organizations.

20 75. NSA employees have also admitting listening to calls simply for their own
21 entertainment -- specifically calls that are in some way tantalizing and salacious -- and sharing the
22 calls of these private, personal conversations with office mates.

23 76. As one former NSA employee, Adrienne Kinne, has explained, NSA
24 interceptors often found themselves listening to "incredibly intimate, personal conversations." She
25 noted, "It's almost like going through and finding somebody's diary."

26 77. Prior to human review, all the acquired communications, including those to,
27 from and/or between Americans, are stored in a vast government database for potential future use.
28 As Director of National Intelligence ("DNI") J. Michael McConnell later explained, immediately

1 after acquisition. "[t]here is no human that is aware of it. So you wouldn't know that until you went
2 into the database." The NSA is currently building a large facility known as the "Utah Data
3 Center," where it is believed these and other communications will be stored in the future. This
4 information is apparently kept indefinitely, even if the subject of the surveillance is an ordinary
5 American. *Trillions* of domestic communications with no intelligence value are acquired and
6 stored in the database.

7 78. On the occasions where the government follows procedures established to
8 protect Americans' privacy (obtaining a warrant or minimization by purging the record from the
9 database), it does so not only after the communications is acquired but only after an analyst reviews
10 the acquired communication. If a government analyst reviewed the communications and
11 determined that "it was a U.S. person inside the United States . . . that would stimulate the system
12 to get a warrant. And that is how the process would work." In other words, the NSA only seeks a
13 warrant (if at all), after the communication is (1) illegally intercepted and acquired; (2) illegally
14 placed in a government database; (3) illegally reviewed by an analyst; and (4) the system flags it
15 for a warrant.

16 79. Under the Spying Program, the NSA engages in "electronic surveillance" as
17 defined by FISA.

18 80. Under the Spying Program, the NSA engages in "interception" of both
19 "wire communication[s]" and "electronic communication[s]" as defined in the Wiretap Act. 18
20 U.S.C. § 2510.

21 81. Under the Spying Program, the NSA intentionally accesses electronic
22 communications without authorization and/or exceeds authorization to access electronic
23 communications that are maintained in "electronic storage" as defined by the SCA.

24 82. Under the Spying Program, the NSA intercepts, searches and seizes, and
25 subjects to electronic surveillance both domestic and international telephone communications of
26 people inside the United States, including citizens and lawful permanent residents, including
27 plaintiffs.

1 83. ... Under the Spying Program, the NSA intercepts, searches and seizes, and ...
2 subjects to electronic surveillance both domestic and international Internet communications,
3 including email, of people inside the United States, including citizens and lawful permanent
4 residents, including plaintiffs, who are innocent, law-abiding citizens have no connection
5 whatsoever to terrorism.

6 84. Under the Spying Program, the NSA has intercepted, subjected to electronic
7 surveillance, and searched and seized millions of both domestic and international telephone and
8 Internet communications (hereinafter collectively "communications") of people inside the United
9 States, including citizens and lawful permanent residents, including plaintiffs. This includes the
10 private phone conversations, private email, and private Internet use of millions of Americans.

11 85. Under the Spying Program, the NSA intercepts, searches and seizes, and
12 subjects to electronic surveillance the communications of people inside the United States without
13 probable cause to believe that the surveillance targets have committed or are about to commit any
14 crime.

15 86. Under the Spying Program, the NSA intercepts, searches and seizes, and
16 subjects to electronic surveillance the communications of people inside the United States without
17 probable cause, reasonable suspicion, or any reason to believe that the surveillance targets either
18 have committed or are about to commit any crime or are foreign powers or agents thereof.

19 87. Under the Spying Program, the NSA intercepts, searches and seizes, and
20 subjects to electronic surveillance the communications of people inside the United States without
21 obtaining specific authorization for each interception from the President or the Attorney General.

22 88. Under the Spying Program, NSA shift supervisors are authorized to approve
23 NSA employees' requests to intercept, search and seize, and subject to electronic surveillance the
24 communications of people inside the United States.

25 89. Under the Spying Program, the NSA does not seek judicial review, obtain a
26 search warrant, a court order, or any lawful authorization whatsoever before or after intercepting,
27 searching and seizing, and subjecting to electronic surveillance the communications of people
28 inside the United States.

1 90. On information and belief, pursuant to the secret Spying Program, the NSA
2 has intercepted, searched and seized, and subjected to electronic surveillance private
3 communications between Americans and their husbands, wives, children, parents, friends, pastors,
4 doctors, lawyers, accountants, and others.

5 91. Each of the named plaintiffs was, pursuant to the Spying Program, subject to
6 the unlawful interception, search and seizure, and electronic surveillance of the contents of their
7 phone and Internet communications.

8 92. Prior to its initiation, defendants never advocated that Congress enact a bill
9 authorizing the illegal Spying Program.

10 93. Prior to its initiation, defendants never sought authorization from the FISA
11 Court to conduct the Spying Program.

12 94. Prior to its initiation, defendants never sought authorization from any Article
13 III Court to conduct the Spying Program.

14 95. Defendants were, or should have been, well aware that the Spying Program
15 was a clear violation of the law.

16 96. Defendants were, or should have been, well aware that the Spying Program
17 is a federal crime.

18 **Recognition of the Blatant Illegality of the Spying Program, and Continued Operations**

19
20 97. The Spying Program was so blatantly illegal that, "when the presidential order
21 was set to expire, the Department of Justice, under Acting Attorney General James Comey, refused
22 to give its approval to the reauthorization of the order because of concerns about the legal basis of
23 certain of these NSA activities." When the-then White House Counsel and Chief of Staff sought
24 approval from Attorney General Ashcroft from his hospital bed, "Ashcroft gave a lucid account of
25 the reasons that Justice had decided to withhold support. And then he went beyond that. Ashcroft
26 said he never should have certified the program. Ashcroft specified a list of facts, and a list of legal
27 concerns, that the secrecy rules had prevented him from discovering. Had he known them, he said,
28 he would have withheld his signature before."

1 98... Despite the apparent conclusion by the Department of Justice that the
2 Program violated criminal laws, President Bush nevertheless reissued the Program Order on or
3 around March 11, 2004. As one author has explained, "Addington deleted the Justice Department
4 from the document [and] typed in 'Alberto R. Gonzales,' the White House Counsel, on a substitute
5 signature line. . . . He did not stop at adding a legally meaningless signature line for Gonzales.
6 Addington drew up new language in which Bush relied upon his own authority to certify the
7 program as lawful." As a result of this incident, about "two dozen Bush appointees," including
8 Acting Attorney General Comey and FBI Director Mueller, were prepared to resign.

9 99. The Spying Program was so blatantly illegal that at least a dozen government
10 officials with knowledge of the Program felt compelled as whistleblowers to report defendants'
11 illegal conduct to *The New York Times*, notwithstanding substantial risks to their employment and
12 potentially to their liberty.

13 100. After the revelations to *The New York Times*, defendant Bush authorized a
14 criminal investigation into the whistleblowing activity.

15 101. To plaintiffs' knowledge, however, defendants have failed to open any
16 criminal investigation into the Spying Program itself.

17 102. In August 2007, Congress passed the Protect America Act of 2007, Public
18 Law 110-55 ("PAA"). Although not authorized by the PAA, the Spying Program continues to this
19 day. As *The Wall Street Journal* noted in March 2008, the essential aspects of the Spying Program
20 are unchanged: "According to current and former intelligence officials, the [NSA] now monitors
21 huge volumes of records of domestic emails and Internet searches as well as bank transfers, credit-
22 card transactions, travel and telephone records. The NSA receives this so-called 'transactional'
23 data from other agencies or private companies, and its sophisticated software programs analyze the
24 various transactions for suspicious patterns."

25

26

27

28

FIRST CAUSE OF ACTION

Foreign Intelligence Surveillance Act, 50 U.S.C. § 1810

(against all Defendants)

103. Plaintiffs repeat and reallege the foregoing paragraphs as if the same were fully set forth at length herein.

104. Plaintiffs are "aggrieved person[s]" as defined in 50 U.S.C. § 1810, are not foreign powers or agents of a foreign power, and were subjected to electronic surveillance conducted or authorized by defendants pursuant to the Spying Program in violation of 50 U.S.C. § 1809.

105. Defendants are "person[s]" within 50 U.S.C. § 1801(m).

106. Plaintiffs are entitled to the damages set forth in 50 U.S.C. § 1810.

SECOND CAUSE OF ACTION

Wiretap Act, 18 U.S.C. §§ 2510, et seq.

(against Defendants Alexander, Hayden, Gonzales and Ashcroft)

107. Plaintiffs repeat and reallege the foregoing paragraphs as if the same were fully set forth at length herein.

108. Plaintiffs are "aggrieved person[s]" as defined in 18 U.S.C. § 2510.

109. The contents of plaintiffs' wire and electronic communications were intercepted by defendants pursuant to the Spying Program in violation of 18 U.S.C. § 2511.

110. Plaintiffs are entitled to the damages set forth in 18 U.S.C. § 2520.

THIRD CAUSE OF ACTION

Stored Communications Act, 18 U.S.C. §§ 2701, *et seq.*

(against Defendants Alexander, Hayden, Gonzales and Ashcroft)

111. Plaintiffs repeat and reallege the foregoing paragraphs as if the same were fully set forth at length herein.

112. Plaintiffs are "aggrieved" within 18 U.S.C. § 2707(a).

113. Defendants intentionally accessed plaintiffs' stored communications without authorization pursuant to the Spying Program in violation of 18 U.S.C. § 2701.

114. Plaintiffs are entitled to the damages set forth in 18 U.S.C. § 2707(c).

FOURTH CAUSE OF ACTION

Bivens/Fourth Amendment

(against all Individual Defendants)

115. Plaintiffs repeat and reallege the foregoing paragraphs as if the same were fully set forth at length herein.

116. By conducting, authorizing, and/or participating in the electronic surveillance of plaintiffs, and by searching and seizing the contents of plaintiffs' communications without reasonable suspicion or probable cause, and failing to prevent their fellow government officers from engaging in this unconstitutional conduct, defendants deprived plaintiffs of rights, remedies, privileges, and immunities guaranteed under the Fourth Amendment of the United States Constitution.

117. In addition, defendants conspired among themselves to deprive plaintiffs of their Fourth Amendment rights, and took numerous overt steps in furtherance of such conspiracy, as set forth above.

1 118. As a direct and proximate result of the misconduct and abuse of authority
2 detailed above, plaintiffs sustained a shocking loss of privacy, and the damages hereinbefore
3 alleged.

4 WHEREFORE, plaintiffs respectfully seek:

5
6 (A) an order certifying this action as a class action pursuant to Fed. R. Civ. P.
7 23(b) for the plaintiff class described herein and naming plaintiffs as the class representatives;

8 (B) a judgment declaring that defendants' Spying Program violates FISA, the
9 Wiretap Act, SCA, and the Fourth Amendment, and permanently enjoining the Spying Program or
10 any NSA electronic surveillance of United States persons without a search warrant or court order,
11 and requiring defendants to delete and destroy, permanently and irrevocably, every communication
12 and record of every communication intercepted by the NSA pursuant to the Spying Program in the
13 custody, control, or possession of the United States or any of its agents or employees;

14 (C) an award of liquidated and/or compensatory damages to the named plaintiffs
15 and members of the class in an amount to be determined at trial;

16 (D) an award of punitive damages to the named plaintiffs and members of the
17 class against the individual defendants in an amount to be determined at trial;

18 (E) an award of reasonable attorneys' fees, costs, and disbursements, pursuant to
19 50 U.S.C. § 1810, 18 U.S.C. § 2520, 18 U.S.C. § 2707, and 28 U.S.C. § 2412.

20 (F) a grant of such other and further relief as this Court shall find just and
21 proper.

22
23
24
25
26
27
28

1 Dated: May 8, 2012

2
3 **EMERY CELLI BRINCKERHOFF**
4 **& ABADY LLP**

5 By: 

6 Ilann M. Maazel

7 Matthew D. Brinckerhoff

8 Adam R. Pulver

9 75 Rockefeller Plaza, 20th Floor

10 New York, N.Y. 10019

11 Phone: (212) 763-5000

12 Fax: (212) 763-5001

13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
Attorneys for Plaintiffs

IN THE UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN FRANCISCO DIVISION

IN RE NATIONAL SECURITY AGENCY
TELECOMMUNICATIONS RECORDS
LITIGATION

MDL Dkt. No. 06-1791-VRW

CLASSIFIED DECLARATION
OF
NATIONAL SECURITY
AGENCY

This Document Relates to:

ALL CASES except *Al-Haramain v. Bush*
(07-109); *CCR v. Bush* (07-1115); *United States*
v. Farber (07-1324); *United States v. Adams*
(07-1326); *United States v. Volz* (07-1396);
United States v. Gaw (07-1242); *Clayton v. AT&T*
Communications of the Southwest (07-1187)

SUBMITTED IN CAMERA,
EX PARTE

Hon. Vaughn R. Walker

Date: November 15, 2007
Time: 2:00 pm
Courtroom: 6 - 17th Floor

I, [REDACTED] do hereby state and declare as follows:

Introduction

1. (U) I am the Deputy Chief of Staff for Operations and Support for the Signals Intelligence Directorate of the National Security Agency (NSA), an intelligence agency within the Department of Defense. I oversee signals intelligence (SIGINT) operations of NSA which includes the SIGINT units of the U.S. armed services. Under Executive Order No. 12333, 46 Fed. Reg. 59941 (1981), as amended on January 23, 2003, 68 Fed. Reg. 4075 (2003), and August 27, 2004, 69 Fed. Reg. 53593 (2004), the NSA SIGINT Directorate is responsible for the collection, processing, and dissemination of SIGINT information for the foreign intelligence purposes of the United States. I am responsible for protecting NSA SIGINT activities, sources and methods against unauthorized disclosures. I have been designated an original TOP SECRET classification authority under Executive Order No. 12958, 60 Fed. Reg. 19825 (1995).

Classified Declaration of [REDACTED]
National Security Agency, *Ex Parte In Camera* Review
MDL No. 06-1791-VRW

1 as amended on March 25, 2003, 68 Fed. Reg. 15315 (2003), and Department of Defense
2 Directive No. 5200.1-R, Information Security Program Regulation, 32 C.F.R. § 159a.12 (2000).
3 I have worked at NSA for thirty three years in various positions as a linguist, analyst and
4 supervisor. As the Deputy Chief of Staff for Operations and Support, I am familiar with the
5 document retention and preservation policies of the NSA.

6 2. ~~(TS//SI)~~ [REDACTED] ~~//TSP//OC/NF~~ I make this declaration in support the
7 United States' Opposition to Plaintiffs' Motion for an Order to Preserve Evidence. The
8 purpose of this declaration is to describe the policies and practices in place at NSA to preserve
9 documents and information related to particular intelligence activities authorized by the
10 President after the 9/11 attacks that are implicated by the claims in this proceeding, as well as to
11 discuss steps that I understand have been taken [REDACTED]
12 [REDACTED]

13 3. ~~(TS//SI)~~ [REDACTED] ~~//TSP//OC/NF~~ I will address the following topics in this
14 declaration. First, I briefly summarize the intelligence activities implicated by these lawsuits
15 and which are subject to the Government's state secrets privilege assertion, as previously in
16 described in the classified Declarations that Lt. General Keith T. Alexander, Director of NSA,
17 has submitted in support of the United States' assertion of the state secrets privilege and NSA
18 statutory privilege in *Hepting v. AT&T*, which involved claims against AT&T, and in the
19 various cases against various *Verizon* defendants (hereafter "*In Camera* Alexander Declaration
20 in *Hepting* Case or *Verizon* Cases"). Second, I identify categories of documents and
21 information that may be related to these activities [REDACTED]
22 [REDACTED]

23 Third, [REDACTED]
24 [REDACTED]

25 1 (U) Classification markings in this declaration are in accordance with the marking system
described in the *In Camera* Alexander Declarations submitted in the *Hepting* and *Verizon* cases.

26 Classified Declaration of [REDACTED]
27 National Security Agency, *Ex Parte In Camera* Review
MDL No. 06-1791-VRW

1 [REDACTED] I then describe the specific preservation status of various categories of documents
2 and information potentially relevant to this litigation.

3 4. (U) My statements in this declaration are based on my personal knowledge of
4 NSA activities as well as information provided to me in the course of my official duties. I have
5 become familiar with the subject matter of the lawsuits before the Court in this action and the
6 Plaintiffs' pending motion. In particular, I have read the Plaintiffs' Motion as well as the
7 classified declarations that General Alexander has submitted, *see supra* ¶ 3

8 5. (TS//SI [REDACTED] ~~//TSP//OC/NF~~) In addition, the description set forth herein
9 of the documents and information maintained and preserved [REDACTED] is
10 known to and has been obtained by NSA in the course of its official duties. As previously
11 described by General Alexander, NSA [REDACTED]
12 [REDACTED] in carrying out its signals intelligence mission.
13 *See In Camera* Alexander Declaration in *Hepting* Case ¶¶ 3, 27-33; *In Camera* Alexander
14 Declaration in *Verizon* Cases ¶¶ 3-4, 24-26. [REDACTED]
15 [REDACTED]
16 [REDACTED]
17 [REDACTED]
18 [REDACTED]
19 [REDACTED]
20 [REDACTED]
21 [REDACTED]
22 [REDACTED]
23 [REDACTED]
24 [REDACTED]
25 [REDACTED]

26 Classified Declaration of [REDACTED]
27 National Security Agency, *Ex Parte In Camera* Review
MDL No. 06-1791-VRW

Summary

6. (TS//SI [REDACTED] //TSP//OC/NF) NSA [REDACTED] taken affirmative steps (described below) to ensure the preservation of information that may be relevant to this litigation. In particular, NSA is preserving a range of documents and communications concerning the presidentially-authorized activities at issue, including: authorizations for these activities by the President; communications [REDACTED] [REDACTED] documents related to the TSP, including specific selectors (e.g., telephone numbers and email addresses) tasked for content interception and the reasons they were targeted; the actual content of communications intercepted under the TSP; intelligence reports containing TSP information; Internet and telephony metadata collected under the Presidential authorization; requests that NSA task that metadata for analysis to obtain information on terrorist contacts [REDACTED] and the reports of that analysis; and miscellaneous information concerning these activities, including legal opinions and analysis relating to the lawfulness of the TSP and metadata activities; briefing materials used to advise Members of Congress and the Foreign Intelligence Surveillance Court about these activities; internal NSA oversight materials, such as NSA Inspector General oversight of the operation of these activities; guidance used by NSA analysts concerning how to designate, use, and protect TSP information in intelligence reports; and technical information concerning the manner in which these presidentially-authorized activities were implemented, [REDACTED]

7. (TS//SI [REDACTED] //TSP//OC/NF) [REDACTED]

Classified Declaration of [REDACTED]
National Security Agency, *Ex Parte In Camera* Review
MDL No. 06-1791-VRW

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

[REDACTED]

Background

A. ~~(TS//SI)~~ ~~_____~~ ~~//TSP//OC/NF~~ NSA Activities

8. ~~(TS//SI)~~ ~~_____~~ ~~//TSP//OC/NF~~ As General Alexander has previously described in detail, the lawsuits before the Court implicate several highly classified and critically important NSA intelligence activities [REDACTED]

As General Alexander explained, this information is subject to the Government's assertion of the state secrets and related statutory privileges and cannot be disclosed without causing exceptionally grave harm to national security. *See In Camera* Alexander Declaration in *Hepting* Case ¶¶ 27-78; *In Camera* Alexander Declaration in *Verizon* Cases ¶¶ 23-90.

² ~~(TS//SI)~~ ~~_____~~ ~~//TSP//OC/NF~~ [REDACTED]

³ ~~(TS//SI)~~ ~~_____~~ ~~//TSP//OC/NF~~ [REDACTED]

Classified Declaration of [REDACTED]
National Security Agency, *Ex Parte In Camera* Review
MDL No. 06-1791-VRW

1 9. ~~(TS//SI [REDACTED] TSP//OC/NF)~~ First, these lawsuits put at issue whether the
2 NSA has intercepted the content of domestic communications of the plaintiffs and other U.S.
3 citizens. As set forth in General Alexander's prior submissions, although the Plaintiffs wrongly
4 allege that the NSA conducts a dragnet of surveillance of the content of millions of
5 communications sent or received by people inside the United States, *see In Camera* Alexander
6 Declaration in *Verizon* Cases at ¶ 54, [REDACTED] the NSA
7 [REDACTED] the interception of the content of communications reasonably believed to
8 involve a member or agent of al Qaeda or an affiliated terrorist organizations pursuant to the
9 President's Terrorist Surveillance Program ("TSP") [REDACTED]

10 [REDACTED]
11 10. ~~(TS//SI [REDACTED] TSP//OC/NF)~~ Second, again after the 9/11 attacks and
12 pursuant to an authorization of the President, [REDACTED] the NSA [REDACTED] the bulk
13 collection of non-content information *about* telephone calls and Internet communications
14 (hereafter "metadata")—activities that enable the NSA to uncover the contacts [REDACTED]
15 [REDACTED] of members or agents of al Qaeda or affiliated terrorist organizations.
16 Specifically, the President authorized the NSA to collect metadata related to *Internet*
17 communications for the purpose of conducting targeted analysis to track al Qaeda-related
18 networks. Internet metadata is header/router/addressing information, such as the "to," "from,"
19 "cc," and "bcc" lines, as opposed to the body or "re" lines, of a standard email. Since July
20 2004, the collection of Internet metadata has been conducted pursuant to an Order of the
21 Foreign Intelligence Surveillance Court ("FISC") authorizing the use of a pen register and trap
22 and trace device ("FISC Pen Register Order"). *See* 18 U.S.C. § 3127 (defining "pen register"
23 and "trap and trace device").

24 11. ~~(TS//SI [REDACTED] TSP//OC/NF)~~ In addition, also after the 9/11 attacks,

25
26 Classified Declaration of [REDACTED]
27 National Security Agency, *Ex Parte In Camera* Review
MDL No. 06-1791-VRW

1 [REDACTED] the NSA [REDACTED] the collection of *telephony* metadata conducted
2 pursuant to an authorization of the President. Such metadata is compiled from call detail data
3 [REDACTED] that reflects non-content
4 information such as the date, time, and duration of telephone calls, as well as the phone
5 numbers used to place and receive the calls. As with the broad Internet metadata collection
6 now authorized by the FISA Court, the bulk collection of telephony metadata was and remains
7 necessary to utilize sophisticated analytical tools for tracking the contacts [REDACTED]
8 [REDACTED] Since May 2006, [REDACTED]
9 have been required to produce this information by order of the FISA Court ("FISC Telephone
10 Records Order").

11 B. ~~(TS//SI//TSP//OC/NF)~~ Document Categories

12 12. ~~(TS//SI)~~ [REDACTED] ~~//TSP//OC/NF)~~ I describe below the categories and
13 preservation status of documents or information maintained by NSA [REDACTED]
14 [REDACTED] in the following three program activities prior to the relevant
15 FISC Order for that activity:⁴

- 16 (i) The Terrorist Surveillance Program authorized by the President to
17 intercept certain international communications into or out of the United
18 States (i.e., "one-end" foreign) that are reasonably believed to involve a
member or agent of al Qaeda or affiliated terrorist organization; and
- 19 (ii) The collection of non-content data concerning Internet
20 communications authorized by the President ("Internet
21 metadata").
- 22 (iii) The collection of telephone calling record information
23 ("telephony metadata") authorized by the President.

24 ⁴ ~~(TS//SI)~~ Because Plaintiffs have not challenged activities occurring pursuant to an order
25 of the FISC, this declaration does not address information collected pursuant to such an
authorization or any retention policies associated therewith.

1 I cannot state that all documents and information concerning these activities have been
2 preserved since the activities commenced under presidential authorization after the 9/11 attacks.
3 I specifically describe below various categories of documents and information concerning these
4 activities that may be potentially relevant to the litigation and that NSA [REDACTED]
5 [REDACTED] acted to preserve since the onset of this litigation.

6 ~~(TS//SI//TSP//OC/NF)~~ Preservation of Information

7 A. ~~(TS//SI)~~ National Security Agency Information

8 13. ~~(TS//SI//TSP//OC/NF)~~ As set forth below, the NSA preserving documents and
9 information potentially relevant to the claims and issues in this lawsuit with respect to the three
10 categories of activities authorized by the President after 9/11 and detailed above for the period
11 prior to the respective superseding FISC orders. NSA has taken various steps to ensure that
12 staff and officials in offices that were cleared to possess information related to the presidentially
13 authorized activities are preserving documents contained in their files and on their computer
14 systems that relate to these activities. Initially, on January 10, 2006, the General Counsel of the
15 National Security Agency, through a classified electronic mail communication, instructed that
16 information, records, or materials (including in electronic form) related to the presidentially-
17 authorized activities be preserved. Prior to the initiation of these lawsuits, NSA has held
18 monthly internal meetings between the Office of General Counsel (OGC), Office of the
19 inspector General, Signals Intelligence Directorate, and senior agency management, to discuss
20 operational and logistical issues associated with the operation of the presidentially-authorized
21 activities; the preservation of information and documents related to those activities has been
22 regularly discussed at these meetings. Following the initiation of these cases in 2006, NSA's
23 OGC has used these meetings to regularly advise the relevant program offices to preserve all
24 information related to these activities, including in electronic form. In addition, in August
25

26 Classified Declaration of [REDACTED]
27 National Security Agency, *Ex Parte In Camera* Review
28 MDL No. 06-1791-VRW

1 2007, following the issuance of Congressional subpoenas for information related to the
2 presidentially-authorized activities, NSA's OGC again instructed the NSA program officials
3 and personnel who had been cleared for access to information concerning the presidentially-
4 authorized activities that all information and documents (including written or electronic) related
5 to these activities and the current litigation be preserved. The categories of documents and
6 information related to the presidentially authorized activities is described below.

7 1. ~~(TS//SI//TSP//OC/NF)~~ [REDACTED]

8 14. ~~(TS//SI//TSP//OC/NF)~~ [REDACTED]

14 15. ~~(TS//SI//TSP//OC/NF)~~ [REDACTED]

17 See

18 *In Camera* Alexander Declaration in *Hepting* Case ¶¶ 61, 74-75; *In Camera* Alexander
19 Declaration in *Verizon* Cases ¶¶ 49-52; and *In Camera* Alexander Declaration in *Shubert* Cases
20 ¶¶ 34-36. Pursuant to the presidential authorization, NSA analysts queried the collected
21 metadata using telephone numbers and email addresses that are reasonably suspected to be
22 associated with al Qaeda or a group affiliated with al Qaeda (as discussed above). [REDACTED]

26 Classified Declaration of [REDACTED]
27 National Security Agency, *Ex Parte In Camera* Review
MDL No. 06-1791-VRW

1 [REDACTED]
2 [REDACTED]
3 [REDACTED]
4 [REDACTED]

Also, as
5 set forth below, NSA has preserved metadata collected in bulk [REDACTED] under
6 presidential authorization.

7 2. ~~(TS//SI//TSP//OC/NF)~~ Presidential Authorizations
8 16. ~~(TS//SI//TSP//OC/NF)~~ NSA is preserving copies of all Presidential
9 authorizations of the TSP and metadata collection activities described herein from the inception
10 of these activities, including the periodic re-authorization of these activities by the President.
11 These authorizations were accompanied by a current analysis of the terrorist threat facing the
12 United States, and these threat memoranda have also been preserved. These documents
13 originated outside of NSA and were obtained and are preserved solely in paper form. These
14 documents are maintained in the offices of the NSA Director.

15 3. ~~(TS//SI//TSP//OC/NF)~~ [REDACTED]
16 17. ~~(TS//SI//TSP//OC/NF)~~ [REDACTED]
17 [REDACTED]
18 [REDACTED]
19 [REDACTED]
20 [REDACTED]

21 4. (U) Terrorist Surveillance Program Information
22 18. ~~(TS//SI//TSP//OC/NF)~~ NSA is preserving several categories of documents
23 related to the Terrorist Surveillance Program under which the content of international, one-end
24 foreign telephone and Internet communications reasonably believed to involve a member or
25

26 Classified Declaration of [REDACTED]
27 National Security Agency, Ex Parte In Camera Review
MDL No. 06-1791-VRW

1 agent of al Qaeda or affiliated terrorist organization were intercepted during the existence of
2 that program. These TSP documents include the following:

3 19. ~~(TS//SI//TSP//OC/NF)~~ TSP Tasking and Probable Cause Information: NSA is
4 preserving documentation assembled by its analysts in the process of determining whether it
5 should, in connection with the TSP, intercept the content of communications of a particular
6 selector (e.g., telephone number or email address). As set forth in General Alexander's prior
7 declarations in this case, the interception of the content of communications under the TSP was
8 triggered by a range of information, including sensitive foreign intelligence, obtained or derived
9 from various sources indicating that a particular phone number or email address is reasonably
10 believed by the U.S. Intelligence Community to be associated with a member or agent of al
11 Qaeda or an affiliated terrorist organization. *See, e.g., In Camera Alexander Declaration in*
12 *Verizon Cases* ¶ 55. After NSA would task for content collection a particular phone number or
13 email address that met this criteria, it preserved documentation of the particular selectors
14 (telephone numbers and Internet addresses) and are reasons for the tasking. [REDACTED]

15 [REDACTED]
16 [REDACTED]
17 [REDACTED]
18 [REDACTED]
19 [REDACTED]
20 [REDACTED]
21 20. ~~(TS//SI//TSP//OC/NF)~~ [REDACTED] NSA preserves
22 documentation on an electronic database of *telephony* selectors tasked (i.e., telephone numbers
23 reasonably believed to be associated with persons outside the United States). Since
24 approximately September 2005, NSA has also maintained a record of foreign Internet selectors
25

26 Classified Declaration of [REDACTED]
27 National Security Agency, *Ex Parte In Camera* Review
MDL No. 86-1791-VRW

1 in an electronic database (which includes the basis for tasking the selector). For the period
2 prior to September 2005, tasking documentation identifying foreign Internet selectors is not
3 complete. However, since the initiation of this lawsuit, NSA has acted to preserve all records
4 that did exist at that time for foreign Internet tasking. ~~_____~~
5 ~~_____~~

6 21. ~~(TS//SI//TSP//OC/NF)~~ TSP Intercepted Content: As described herein, NSA is
7 preserving the actual content of communications intercepted under the presidentially-authorized
8 TSP as described in this paragraph. For voice intercepts under the TSP, NSA has maintained
9 all "raw traffic" in an electronic database.⁵ From the initiation of the TSP until the program
10 ceased in 2007, the raw traffic of Internet content intercepts were maintained on a database for
11 approximately 180 days. Because the operational relevance of this intelligence declined over
12 time, and because the performance of this system is affected by the volume maintained on the
13 online database, NSA migrated the raw Internet traffic to computer tape. However, NSA is
14 preserving tapes of the Internet content intercepted under the TSP since the inception of the
15 program.

16 22. ~~(TS//SI//TSP//OC/NF)~~ Intelligence Reports: NSA analysts have prepared
17 detailed intelligence reports that utilize content intercepts obtained under the TSP authorization
18 by the President. NSA intelligence reports are written assessments of intelligence on particular
19 topics (for example, the threat of al Qaeda attacks or the activities of suspected al Qaeda
20 operatives). For each of these reports, an NSA analyst is able to determine if information
21 obtained through a TSP intercept was utilized. All NSA intelligence reports are preserved
22 ~~_____~~

23 ⁵ ~~(TS//SI//TSP//OC/NF)~~ Due to a technical malfunction (which occurred on or about
24 January 26, 2007), raw telephony intercept for a period of approximately six months (June
25 2005-December 2005) was inadvertently deleted from this database. However, foreign
intelligence information derived from these raw intercepts is preserved.

26 Classified Declaration of ~~_____~~
27 National Security Agency, *Ex Parte In Camera* Review
MDL No. 06-1791-VRW

1 permanently in paper and electronic form.

2 5. ~~(TS//SI//TSP//OC/NF)~~ Internet and Telephony Metadata Collection

3 23. ~~(TS//SI//TSP//OC/NF)~~ Internet Metadata Collection: As described
4 above and in General Alexander's prior Declarations, starting in October 2001, and now
5 pursuant to the FISC Pen Register Order, NSA has obtained [REDACTED]

6 [REDACTED] bulk metadata associated with electronic communications [REDACTED]
7 [REDACTED]
8 [REDACTED]
9 [REDACTED]

10 *See, e.g., In Camera Alexander Declaration in Verizon Cases*, ¶ 31. NSA collected
11 Internet metadata pursuant to Presidential authorization until [REDACTED] 2004 (nearly two years
12 before these lawsuits commenced). On [REDACTED] 2004, NSA took initial steps to embargo this
13 data from access by all NSA analysts. Because the Internet metadata collected prior to the FISC
14 order was no longer being used for analysis, it was migrated to electronic tapes starting in
15 January 2006. Those tapes are stored by the Signals Intelligence Directorate. To be clear, the
16 presidentially authorized collection of internet metadata is segregated from information
17 collected under the FISC Order of July 2004 and has not been destroyed.

18 24. ~~(TS//SI//TSP//OC/NF)~~ Telephony Metadata Collection: As
19 described above and in General Alexander's prior declarations, starting in October 2001, and
20 now pursuant to the FISC Telephone Records Order entered in May 2006 (FISC Telephone
21 Records Collection Order), NSA has collected [REDACTED]
22 telephony metadata compiled from call detail records that [REDACTED]
23 [REDACTED] reflects non-content information such as the date, time, and duration
24 of telephone calls, as well as the phone numbers used to place and receive the calls. *See, e.g.,*
25

26 Classified Declaration of [REDACTED]
27 National Security Agency, *Ex Parte In Camera Review*
MDL No. 06-1791-VRW

1 *In Camera* Alexander Declaration in *Verizon* Cases ¶ 32. The telephony metadata NSA
2 collected [REDACTED] prior to the FISC order is segregated in an online database from that
3 collected after May 2006 under the FISC Order, but remains subject to querying for analysis of
4 [REDACTED] contacts by those reasonably believed to be associated with al
5 Qaeda and affiliated terrorist organizations.

6 25. ~~(TS//SI)~~ [REDACTED] ~~//TSP//OC/NF~~ For operational reasons, NSA maintains
7 approximately five years worth of telephony metadata in its online database. Data acquired
8 after 2003 under Presidential authorization is preserved electronically in an online data base.
9 NSA has migrated to tapes telephony metadata collected during the period 2001-02, since the
10 current operational relevance of that data has declined and continuing to maintain it on current
11 operational systems would be unnecessary and would encumber current operations with more
12 recent data. NSA's operational policy is to continue to migrate telephony metadata beyond five
13 years old from an online database to tapes for preservation. To the extent NSA is required to
14 halt the migration of older telephony metadata to tape, less relevant data would be retained in
15 the operational system, encumbering the performance of the current online database because of
16 the volume of data, and this would severely undermine NSA's ability to identify [REDACTED]
17 contacts of suspected terrorist communications.

18 26. ~~(TS//SI)~~ [REDACTED] ~~//TSP//OC/NF~~ Information Pertaining to Queries of Meta-Data: NSA is
19 preserving documentation of requests that it query its database of Internet and telephony
20 metadata for analysis. See *In Camera* Alexander Declaration in *Verizon* Cases ¶¶ 31-32 and *In*
21 *Camera* Alexander Declaration in *Hepting* Cases ¶¶ 37-43 (describing contact chaining [REDACTED]
22 [REDACTED] of metadata). This documentation indicates the selectors (Internet addresses
23 and phone numbers) that NSA searched in order to analyze particular contacts [REDACTED]
24 [REDACTED] for that selector, and the basis for its analysis for the selectors under which the
25

26 Classified Declaration of [REDACTED]
27 National Security Agency, *Ex Parte In Camera* Review
MDL No. 06-1791-VRW

1 metadata was queried. Documentation of metadata queries is maintained by NSA's Signals
2 Intelligence Directorate in electronic form.

3 27. ~~(TS//SI//TSP//OC/NF)~~ Reports of Metadata Analysis: NSA is preserving
4 documentation of its analysis of Internet and Telephony Metadata obtained pursuant to
5 Presidential authorization and prior to the respective FISC Orders for these activities. These
6 reports include the results of any contact chaining [REDACTED] for particular selectors
7 reasonably believed to be that of a member or agent of al Qaeda or affiliated terrorist
8 organization. This documentation sets forth NSA's assessment of a particular Internet or
9 telephony selector's contacts [REDACTED] in order to detect other potential al
10 Qaeda associates. Reports documenting metadata analysis are maintained by NSA's Signals
11 Intelligence Directorate in both an electronic database and in paper form.

12 6. ~~(TS//SI)~~ Miscellaneous NSA Information

13 28. ~~(TS//SI)~~ [REDACTED] ~~//TSP//OC/NF)~~ As summarized below, NSA is also preserving
14 miscellaneous categories of administrative records related to the presidentially-authorized
15 activities implicated by these lawsuits (TSP content collection, Internet metadata collection,
16 telephony metadata collection). These categories include:

- 17 (i) Legal Opinions and analysis relating to the lawfulness of the TSP and metadata
18 activities. This information is maintained in paper form in the Office of the General
19 Counsel.
- 20 (ii) Materials Related to Briefings to Members of Congress and the FISA Court on the TSP
21 and metadata activities since their inception. These documents are being maintained
22 and preserved in paper form by the Program Manager's Office for these NSA activities.
23 In addition, an electronic version of the latest iteration of these briefings is also
24 maintained. Although no briefing materials have been destroyed since the initiation of
25 these lawsuits in 2006, it is possible that not all earlier iterations of briefings have been
26 preserved.
- 27 (iii) NSA Internal Oversight Documents of the presidentially-authorized TSP and metadata
28 collection activities, including reports by the NSA General Counsel and the NSA
Inspector General of the operation of these activities. NSA also is preserving agendas
and notes of regular monthly meetings between the Office of the General Counsel,

26 Classified Declaration of [REDACTED]
27 National Security Agency, *Ex Parte In Camera* Review
MDL No. 06-1791-VRW

Office of the Inspector General, and the Signals Intelligence Directorate, which review and address legal and operational issues concerning the TSP and metadata collection activities described herein.

- (iv) Classification Guides that address the classification status, processing, dissemination, and reporting of intelligence traffic and information obtained pursuant to the presidential authorization. This guidance, which NSA intelligence analysts use in analyzing TSP traffic, includes instructions on how to designate and protect TSP information in intelligence reports, how to designate its classification status, and how to implement NSA minimization procedures in drafting reports (typically procedures that require the minimization of the names of U.S. persons mentioned in such reports who are not foreign intelligence targets). This information is maintained in electronic form.
- (v) Technical Information concerning the manner in which presidentially-Authorized activities were implemented. [REDACTED] such as technical proposals, and technical plans for undertaking particular tasks.

Classified Declaration of [REDACTED]
National Security Agency, *Ex Parte In Camera* Review
MDL No. 06-1791-VRW

~~TOP SECRET//COMINT~~ [REDACTED] ~~//TSP//ORCON//NOFORN//MR~~

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28



Classified Declaration of [REDACTED]
National Security Agency, *Ex Parte In Camera* Review
MDL No. 06-1791-VRW

~~TOP SECRET//COMINT~~ [REDACTED] ~~//TSP//ORCON//NOFORN//MR~~

~~TOP SECRET//COMINT [REDACTED] TST//ORCON/NOFORN//MR~~

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

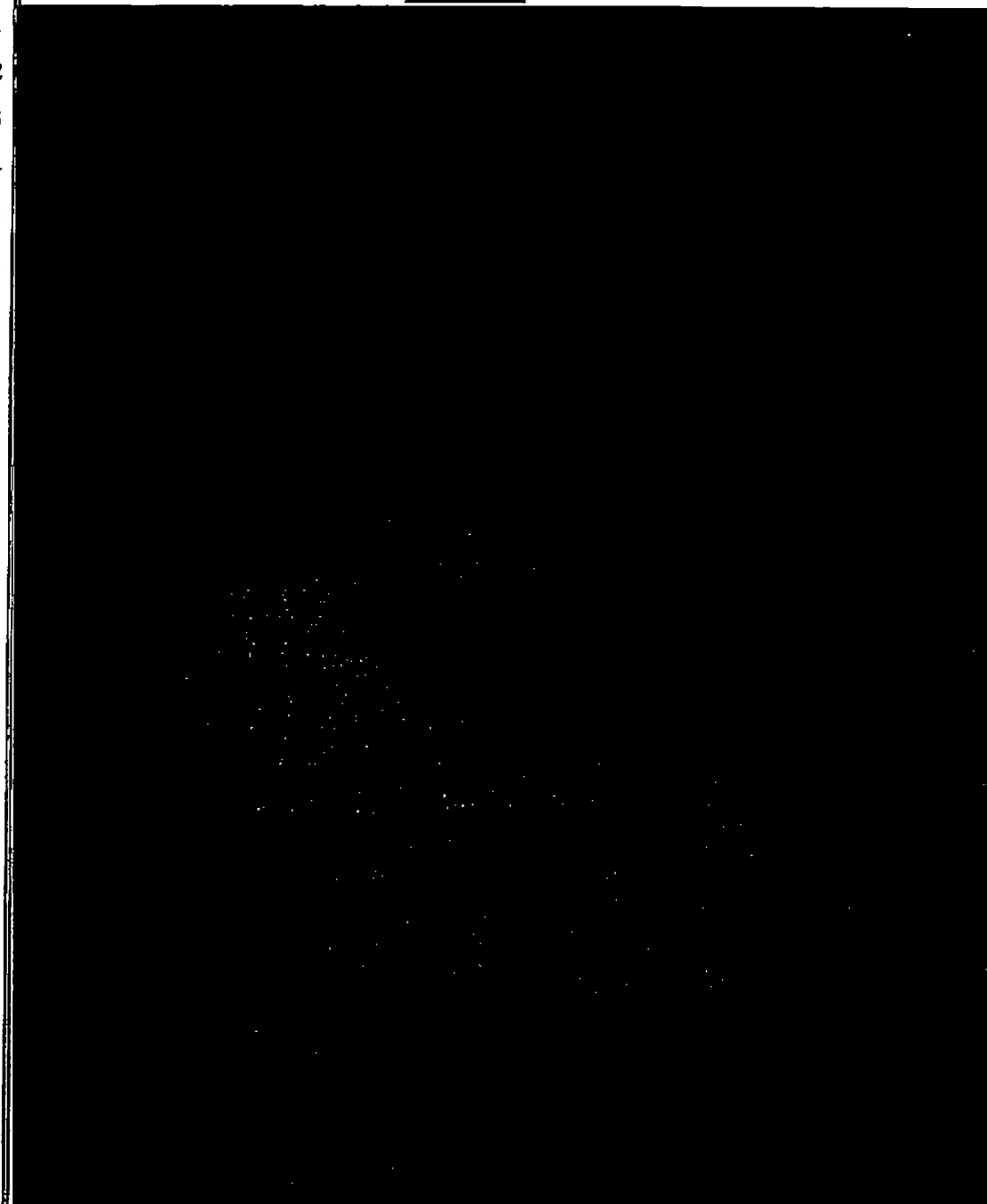


Classified Declaration of [REDACTED]
National Security Agency, *Ex Parte In Camera* Review
MDL No. 06-1791-VRW

~~TOP SECRET//COMINT [REDACTED] TST//ORCON/NOFORN//MR~~

~~TOP SECRET//COMINT~~ [REDACTED] ~~//TSP//ORCON/NOFORN//MR~~

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28



Classified Declaration of [REDACTED]
National Security Agency, *Ex Parte In Camera* Review
MDL No. 06-1791-VRW

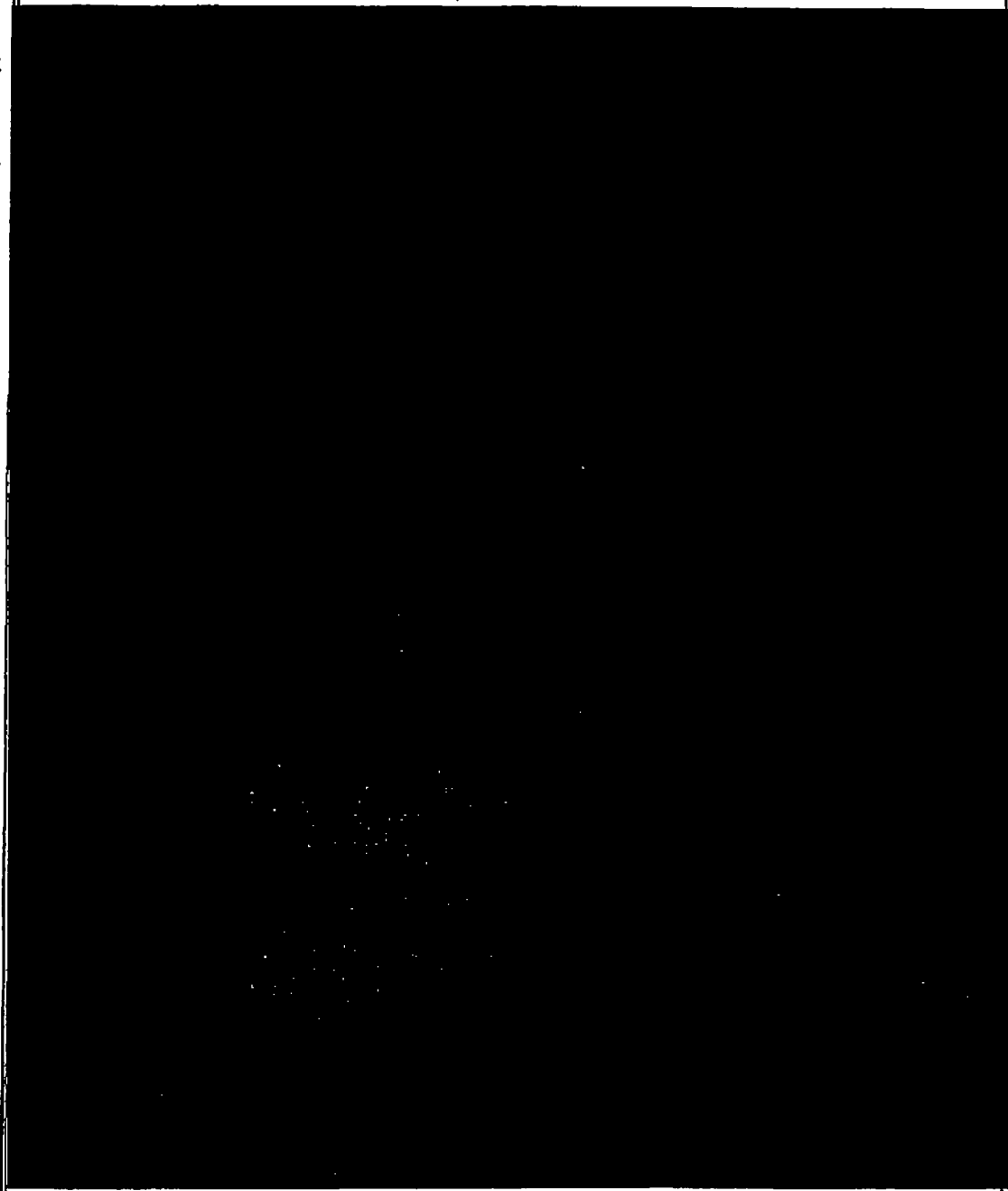
~~TOP SECRET//COMINT~~ [REDACTED] ~~//TSP//ORCON/NOFORN//MR~~

1 [REDACTED]
2 [REDACTED]
3 [REDACTED]
4 [REDACTED]
5 [REDACTED]
6 [REDACTED]
7 [REDACTED]
8 [REDACTED]
9 [REDACTED]
10 [REDACTED]
11 [REDACTED]
12 [REDACTED]
13 [REDACTED]
14 [REDACTED]
15 [REDACTED]
16 [REDACTED]
17 [REDACTED]
18 [REDACTED]
19 [REDACTED]
20 [REDACTED]
21 [REDACTED]
22 [REDACTED]
23 [REDACTED]
24 [REDACTED]
25 [REDACTED]

26 Classified Declaration of [REDACTED]
27 National Security Agency, *Ex Parte In Camera* Review
MDL No. 06-1791-VRW

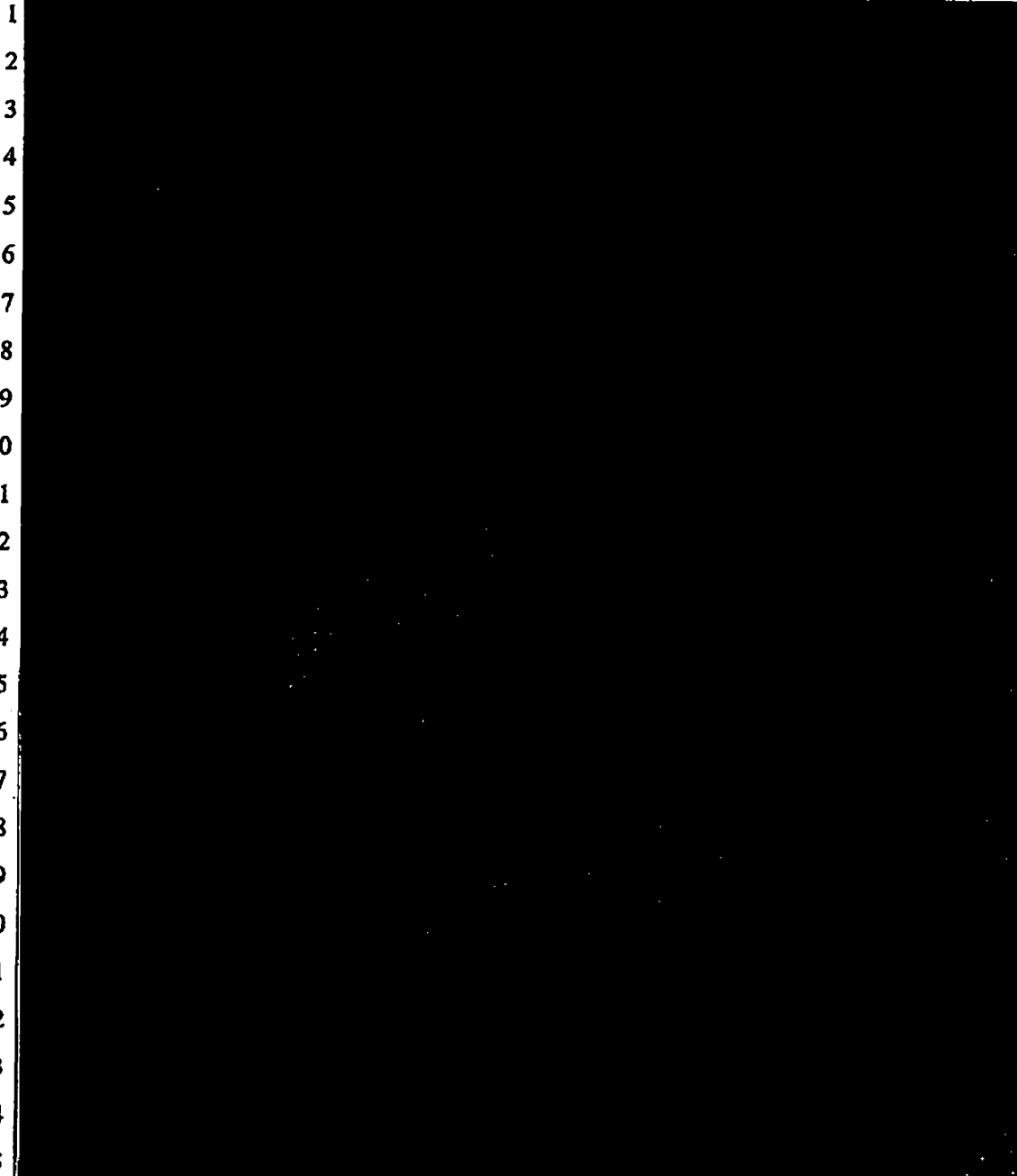
~~TOP SECRET//COMINT [REDACTED]//TST//ORCON/NOFORN//MR~~

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28



Classified Declaration of [REDACTED]
National Security Agency, *Ex Parte In Camera* Review
MDL No. 06-1791-VRW

~~TOP SECRET//COMINT [REDACTED]//TST//ORCON/NOFORN//MR~~

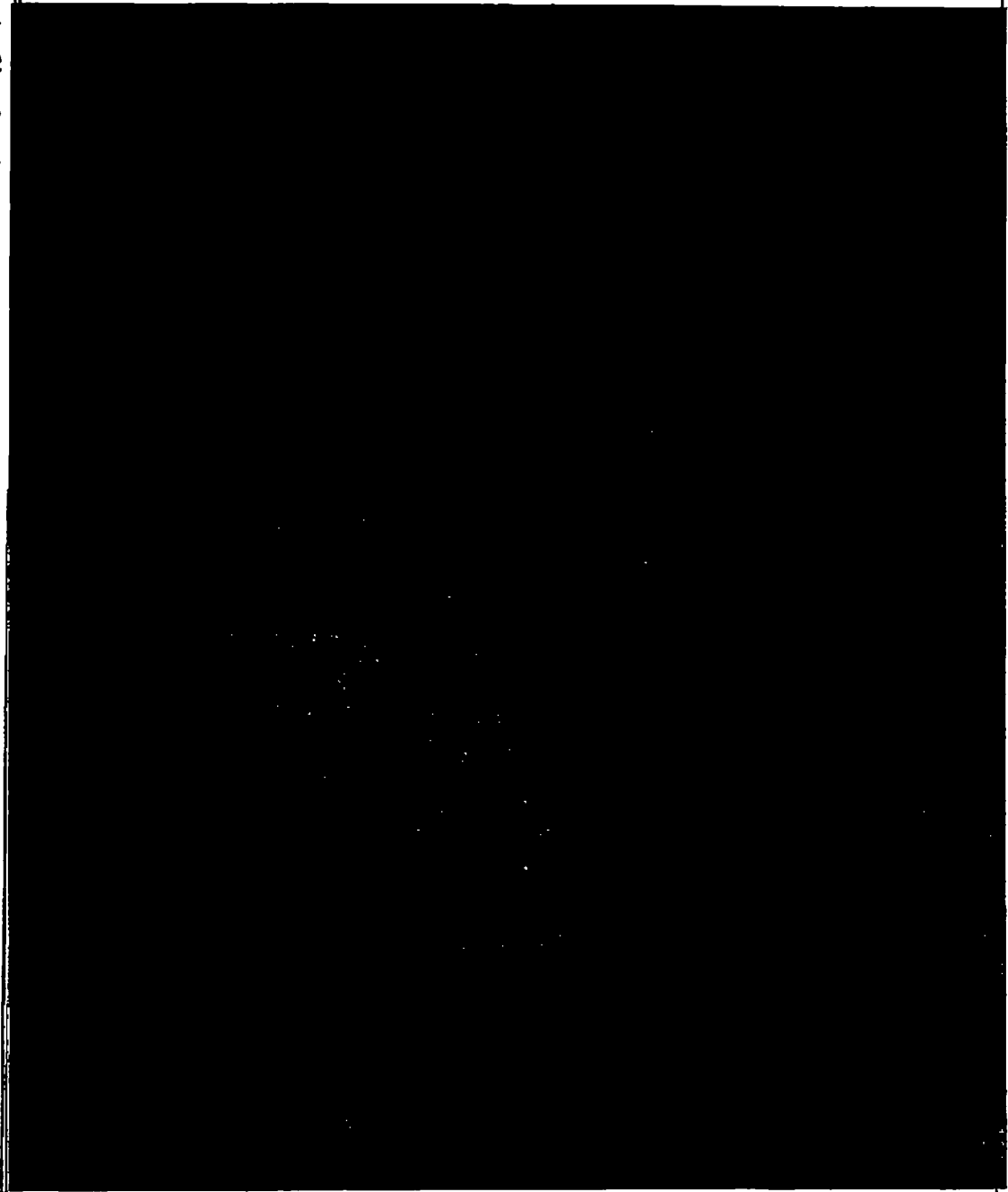


1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

Classified Declaration of [REDACTED]
National Security Agency, *Ex Parte In Camera* Review
MDL No. 06-1791-VRW

~~TOP SECRET//COMINT~~ [REDACTED] ~~//TSP//ORCON//NOFORN//MR~~

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28



Classified Declaration of [REDACTED]
National Security Agency, *Ex Parte In Camera* Review
MDL No. 06-1791-VRW

~~TOP SECRET//COMINT~~ [REDACTED] ~~//TSP//ORCON//NOFORN//MR~~

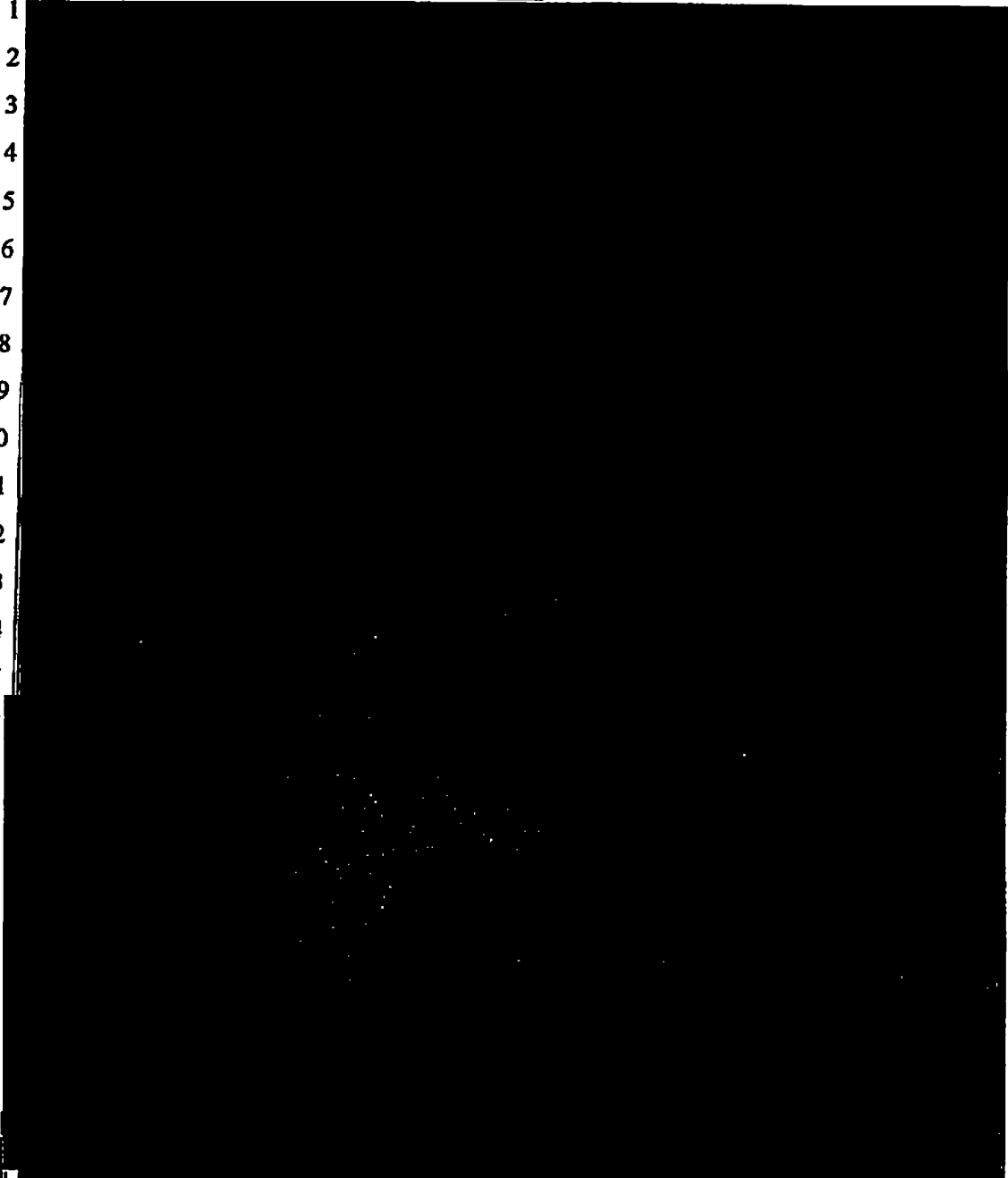
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28



Classified Declaration of [REDACTED]
National Security Agency, *Ex Parte In Camera* Review
MDL No. 06-1791-VRW

~~TOP SECRET//COMINT [REDACTED]//TSP//ORCON/NOFORN//MR~~

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28



Classified Declaration of [REDACTED]
National Security Agency, *Ex Parte In Camera* Review
MDL No. 06-1791-VRW

~~TOP SECRET//COMINT [REDACTED]//TSP//ORCON/NOFORN//MR~~

[REDACTED]

* * *

54. (U) If the Court has any questions concerning this submission, the NSA is prepared to address them and assist the Court further through secure *in camera*, *ex parte*

Classified Declaration of [REDACTED]
National Security Agency, *Ex Parte In Camera* Review
MDL No. 06-1791-VRW

~~TOP SECRET//COMINT~~ [REDACTED] ~~//TSP//ORCON//NOFORN//MR~~

1 proceedings.

2 I declare under penalty of perjury that the foregoing is true and correct.

3
4 DATE: 25 October 2007

5 [REDACTED]
6 [REDACTED]
7 Deputy Chief of Staff for Operations and Support
8 Signals Intelligence Directorate
9 National Security Agency
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25

26 Classified Declaration of [REDACTED]
27 National Security Agency, *Ex Parte In Camera* Review
MDL No. 06-1791-VRW

28 ~~TOP SECRET//COMINT~~ [REDACTED] ~~//TSP//ORCON//NOFORN//MR~~