

# Exhibit 15

# United States Senate

WASHINGTON, DC 20510

March 15, 2012

The Honorable Eric Holder  
Attorney General  
United States Department of Justice  
Washington, D.C. 20530

Dear Attorney General Holder:

We have discussed the dangers of relying on secret interpretations of public laws with you on multiple occasions, both through correspondence and in person. While we know that you are generally aware of our views on this subject, we feel obliged to comment specifically on the Justice Department's recent attempt to seek dismissal of two lawsuits that have been filed under the Freedom of Information Act and that specifically pertain to this problem of secret law.

The two lawsuits (filed by the New York Times and the American Civil Liberties Union) seek to obtain information about how the United States government has interpreted the text of the USA Patriot Act, specifically section 215 of that Act, the controversial "business records" provision.

It is a matter of public record that section 215, which is a public statute, has been the subject of secret legal interpretations. The existence of these interpretations, which are contained in classified opinions issued by the Foreign Intelligence Surveillance Court (or "FISA Court") has been acknowledged on multiple occasions by the Justice Department and other executive branch officials.

We believe most Americans would be stunned to learn the details of how these secret court opinions have interpreted section 215 of the Patriot Act. As we see it, there is now a significant gap between what most Americans think the law allows and what the government secretly claims the law allows. This is a problem, because it is impossible to have an informed public debate about what the law should say when the public doesn't know what its government thinks the law says.

As we have said before, we believe that it is entirely legitimate for government agencies to keep certain information secret. Americans acknowledge that their government can better protect national security if it is sometimes allowed to operate in secrecy and as such, they do not expect the Obama Administration to publish every detail about how intelligence is collected any more than early Americans expected George Washington to tell them his plans for observing troop movements at Yorktown. However, in a democratic society – in which the government derives its power from the consent of the people – citizens rightly expect that their government will not arbitrarily keep information from them. Americans expect their government to operate within the boundaries of publicly-understood law, and as voters they have a need and a right to

know how the law is being interpreted, so that they can ratify or reject decisions made on their behalf. To put it another way, Americans know that their government will sometimes conduct secret operations, but they don't think that government officials should be writing secret law.

While the executive branch has worked hard to keep the government's official interpretation of the Patriot Act secret from the American public it has, to its credit, provided this information in documents submitted to Congress. However, these documents are so highly classified that most members of Congress do not have any staff who are cleared to read them. As a result, we can state with confidence that most of our colleagues in the House and Senate are unfamiliar with these documents, and that many of them would be surprised and angry to learn how the Patriot Act has been interpreted in secret.

A number of the senators who are familiar with these secret legal interpretations (including the two of us) have pressed the executive branch to declassify these interpretations so that Congress and the public can have an informed debate about the proper scope of the law. We have personally raised this issue in meetings, hearings, and correspondence (both classified and unclassified) with senior officials (including you) on many occasions over the years, thus far to no avail. It was initially encouraging when the Department of Justice and the Office of the Director of National Intelligence wrote to Senator Rockefeller and Senator Wyden in August 2009 to announce the establishment of a regular process for reviewing, redacting and releasing significant opinions of the FISA Court. Two and a half years later, however, this "process" has produced literally zero results. Not a single redacted opinion has been released.

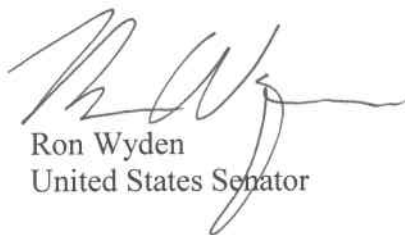
The crux of the Justice Department's argument for keeping the official interpretation of the law secret is that this secrecy prevents US adversaries from understanding exactly what intelligence agencies are allowed to do. We can see how it might be tempting to latch on to this chilling logic, but we would note that it would then follow that all of America's surveillance laws should be secret, because that would make it even harder to guess how the United States government collects information. For example, when Congress passed the Foreign Intelligence Surveillance Act in 1978 it would have been useful to keep that law secret from the KGB, so that Soviet agents would not know how the FBI was allowed to track them. But American laws should not be made public only when government officials find it convenient. They should be public all the time, and every American should be able to find out what their government thinks those laws mean. We recognize that this obligation to be transparent with the public can be a challenge, but avoiding that challenge by developing a secret body of law is not an acceptable solution.

The Justice Department's motion to dismiss these Freedom of Information Act lawsuits argues that it is the responsibility of the executive branch to determine the best way to protect the secrecy of intelligence sources and methods. While this is indeed a determination for the executive branch to make, we are concerned that the executive branch has developed a practice of bypassing traditional checks and balances and treating these determinations as dispositive in all cases. In other words, when intelligence

officials argue that something should stay secret, policy makers often seem to defer to them without carefully considering the issue themselves. We have great respect for our nation's intelligence officers, the vast majority of whom are hard-working and dedicated professionals. But intelligence officials are specialists – it is their job to determine how to collect as much information as possible, but it is not their job to balance the need for secrecy with the public's right to know how the law is being interpreted. That responsibility rests with policy makers, and we believe that responsibility should not be delegated lightly.

We would also note that in recent months we have grown increasingly skeptical about the actual value of the "intelligence collection operation" discussed in the Justice Department's recent court filing regarding the pending lawsuits. This has come as a surprise to us, as we were initially inclined to take the executive branch's assertions about the importance of this "operation" at face value. We will provide more detail about this skepticism in classified correspondence.

We hope that you will reconsider the Justice Department's stance on the issue of secret legal interpretations, as we continue to believe that this stance is contrary to core principles of American democracy and will serve our nation quite poorly over the long term. Thank you for your attention to this matter.



Ron Wyden  
United States Senator

Sincerely,



Mark Udall  
United States Senator

# Exhibit 16

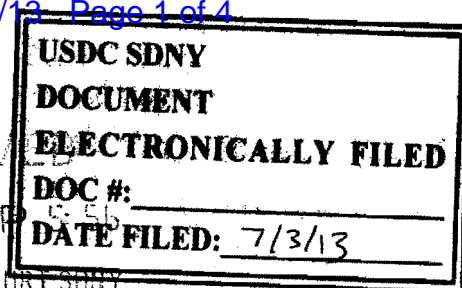


(TS//SI//NF) FAA Certification Renewals With Caveats  
By [REDACTED] on 2011-10-12 0850

(TS//SI//NF) The FISA Court signed the 2011 FAA Certifications on 3 Oct 2011 – these are valid until 2 Oct 2012, permitting SSO FAA-authorized accesses to continue operations. However, in the 80-page opinion, the judge ordered certain “upstream” or “passive” FAA DNI collection to cease after 30 days, unless NSA implements solutions to correct all deficiencies identified in the opinion document. PRISM operations are not affected by these caveats. All PRISM providers, except Yahoo and Google, were successfully transitioned to the new Certifications. We expect Yahoo and Google to complete transitioning by Friday 6 Oct. Regarding the non-PRISM FAA collection programs, the Court cited targeting and minimization procedures related to collection of Multiple Communications Transactions as “deficient on statutory and constitutional grounds.” SSO, Technology Directorate, OGC, and other organizations are coordinating a response, which includes planning to implement a conservative solution in which the higher-risk collection will be sequestered. It is possible that this higher risk collection contains much of the non-duplicative FAA collection resulting in FAA reporting from upstream accesses. This solution is designed to comply with the judge’s order; however, the judge will have to determine if it does. If the solution is installed, SSO will then work with OPIs and OGC to modify the solution over time such that the filtering process will be optimized to permit more valid collection to be processed and forwarded to OPIs. Finally, in parallel with these efforts, the OGC is contemplating filing an appeal to the ruling.

# Exhibit 17

JAMEEL JAFFER  
DEPUTY LEGAL DIRECTOR



RECEIVED

2013 JUL -2 P 6:55

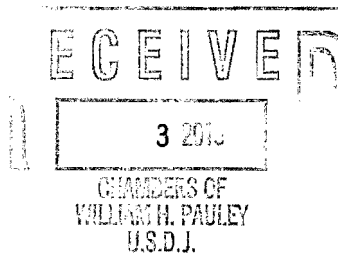
U.S. DISTRICT COURT SDNY  
July 2, 2013

MEMO ENDORSED

Handwritten initials/signature

BY HAND

Honorable William H. Pauley III  
United States District Court for the  
Southern District of New York  
500 Pearl Street, Room 2210  
New York, NY 10007



AMERICAN CIVIL LIBERTIES  
UNION FOUNDATION  
NATIONAL OFFICE  
125 BROAD STREET, 18TH FL.  
NEW YORK, NY 10004-2400  
T/212.549.2500  
WWW.ACLU.ORG

Re: *American Civil Liberties Union et al. v. Clapper et al.*  
Case No. 13-CV-03994 (WHP) (JLC)

Dear Judge Pauley:

OFFICERS AND DIRECTORS  
SUSAN N. HERMAN  
PRESIDENT

ANTHONY D. ROMERO  
EXECUTIVE DIRECTOR

On behalf of Plaintiffs, who challenge the lawfulness of the government's dragnet acquisition of "metadata" relating to every phone call made or received by residents of the United States, we write to request a pre-motion conference to discuss a motion for a preliminary injunction. Because the Court has already scheduled an initial conference in this matter for July 17, we respectfully request that the Court also conduct the pre-motion conference on that date.

By way of background, on June 5, 2013, *The Guardian* published a story reporting that the National Security Agency ("NSA") was "collecting the telephone records of millions of US customers of Verizon, one of America's largest telecoms providers." Glenn Greenwald, *NSA Collecting Phone Records of Millions of Verizon Customers Daily*, *Guardian*, June 5, 2013, <http://gu.com/p/3gc62/tw>. *The Guardian* also published an order of the Foreign Intelligence Surveillance Court ("FISC") directing Verizon Business Network Services ("VBNS") to "produce to the [NSA] . . . and continue production on an ongoing daily basis thereafter . . . all call detail records or 'telephony metadata' created by Verizon for communications (i) between the United States and abroad; or (ii) wholly within the United States, including local telephone calls" over the three-month period ending on July 19, 2013.

The government has since authenticated the VBNS order. James R. Clapper, DNI Statement on Recent Unauthorized Disclosures of Classified Information (June 6, 2013), <http://1.usa.gov/188X5LW>. Senator Diane Feinstein, who chairs the Senate Select Committee on Intelligence, has disclosed that the VBNS order was part of a broader program that has been in



place for seven years, and that similar orders have been served on all of the major telephone companies. *Senator Feinstein: NSA Phone Call Data Collection in Place 'Since 2006,'* Guardian, June 6, 2013, <http://bit.ly/13rfxdu>.

As alleged in the Complaint, Plaintiffs are current and former VBNS subscribers. The VBNS order requires VBNS to turn over to the government, on an “ongoing daily basis,” all metadata associated with Plaintiffs’ phone calls. Under the VBNS order and predecessor orders, the government has collected detailed information about Plaintiffs’ communications and stored that information in government databases. The government’s past and ongoing collection of this information allows it to learn sensitive and privileged information about Plaintiffs’ work and clients, and it is likely to have a chilling effect on whistleblowers and others who might otherwise contact Plaintiffs for legal assistance.

AMERICAN CIVIL LIBERTIES  
UNION FOUNDATION

The government’s surveillance of Plaintiffs’ communications is not authorized by Section 215 of the Patriot Act, 18 U.S.C. § 1861, the provision under which the VBNS order was issued, and it violates the First and Fourth Amendments. Plaintiffs have filed this suit to obtain a declaration that this surveillance is unlawful; to enjoin the government from continuing the surveillance under the VBNS order or any successor thereto; and to require the government to purge from its databases all of the call records related to Plaintiffs’ communications collected pursuant to the VBNS order or any predecessor thereto.

Plaintiffs intend to file a motion for a preliminary injunction (i) directing the government to quarantine all of Plaintiffs’ telephony metadata collected under the VBNS order or any predecessor or successor thereto; and (ii) barring the government from querying metadata obtained through the VBNS order using any phone number or other identifier associated with the Plaintiffs.

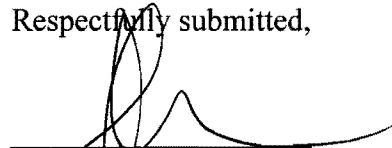
Preliminary relief is warranted here. The harm suffered by Plaintiffs is ongoing and irreparable. Plaintiffs are non-profit organizations engaged in public education, lobbying, and pro bono litigation concerning civil rights and civil liberties. The tracking and retention of their telephony metadata with respect to every call they make or receive is a direct and wide-ranging invasion of their constitutional right to privacy. This continuing invasion is, by itself, irreparable injury. *See, e.g., Covino v. Patrissi*, 967 F.2d 73, 77 (2d Cir. 1992). Equally irreparable, and equally substantial, is the injury to Plaintiffs’ expressive and associational rights. *See Brown v. Socialist Workers '74 Campaign Comm. (Ohio)*, 459 U.S. 87, 96–98 (1982); *Elrod v. Burns*, 427 U.S. 347, 373 (1976).

Plaintiffs will also show a substantial likelihood of success on the merits. First, the surveillance under the VBNS order is not authorized by Section 215. That provision does not authorize the government to collect everything; it authorizes the collection of records that are “relevant” to authorized investigations. In addition, Section 215 authorizes the collection of “tangible things” already in existence; it does not authorize the government to order recipients to turn over records as they are generated. Indeed, as Plaintiffs will demonstrate, reading the provision to permit the latter kind of surveillance makes nonsense of the larger statutory scheme.

The surveillance under the VBNS order is also unconstitutional. The kind of information being collected by the government is highly sensitive, and its warrantless and suspicionless collection over long periods constitutes an unreasonable search under the Fourth Amendment. *Cf. United States v. Jones*, 132 S. Ct. 945 (2012) (holding that tracking of location data for one individual over twenty-eight days constituted a search under the Fourth Amendment). It also violates the First Amendment by exposing private association to government scrutiny and by substantially burdening Plaintiffs’ protected advocacy and expression. *See Gibson v. Fla. Legis. Investigation Comm.* 372 U.S. 539, 546 (1963); *NAACP v. Ala. ex rel. Patterson*, 357 U.S. 449, 460–61 (1958); *McIntyre v. Ohio Elections Comm’n*, 514 U.S. 334, 347 (1995).

Finally, the balance of hardships favors Plaintiffs’ request for preliminary relief. The preliminary injunction sought by Plaintiffs would substantially mitigate the continuing violation of Plaintiffs’ rights. At the same time, entry of the requested injunction would not prejudice any legitimate government interest. Should Plaintiffs not ultimately prevail, the government will be in the same position it would have been in had Plaintiffs’ suit never been brought. Pending final judgment, the government can access Plaintiffs’ telephony metadata, if necessary, under a proper demonstration of cause under other authorities. *See, e.g.*, 50 U.S.C. § 1842 (authorizing pen registers in foreign intelligence investigations).

Respectfully submitted,



Jameel Jaffer  
Alex Abdo  
Brett Max Kaufman  
Patrick Toomey  
Catherine Crump  
American Civil Liberties Union  
Foundation  
125 Broad Street, 18th Floor  
New York, NY 10004  
Phone: (212) 549-2500  
Fax: (212) 549-2654  
jjaffer@aclu.org

*Counsel for Plaintiffs*


Christopher T. Dunn  
Arthur N. Eisenberg  
New York Civil Liberties Union  
Foundation  
125 Broad Street, 19th Floor  
New York, NY 10004  
Phone: (212) 607-3300  
Fax: (212) 607-3318  
aeisenberg@nyclu.org

AMERICAN CIVIL LIBERTIES  
UNION FOUNDATION

Cc: Tara Marie La Morte  
(tara.lamorte2@usdoj.gov)

Application granted. The Court will hold a pre-motion conference in conjunction with the initial pre-trial conference, which has been rescheduled to July 25, 2013 at 12:00 p.m.

SO ORDERED:



WILLIAM H. PAULEY III U.S.D.J. 7/3/13

# Exhibit 18

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



Honorable Reggie B. Walton  
Presiding Judge

July 29, 2013

Honorable Patrick J. Leahy  
Chairman  
Committee on the Judiciary  
United States Senate  
Washington, DC 20510

Dear Mr. Chairman:

I am writing in response to your letter of July 18, 2013, in which you posed several questions about the operations of the Foreign Intelligence Surveillance Court (the Court). As you requested, we are providing unclassified responses. We would note that, as a general matter, the Court's practices have evolved over time. Various developments in the last several years – including statutory changes, changes in the size of the Court and its staff, the adoption of new Rules of Procedure in 2010, and the relocation of the Court's facilities from the Department of Justice headquarters to a secure space in the federal courthouse in 2009 – have affected some of these practices. The responses below reflect the current practices of the Court.

1. *Describe the typical process that the Court follows when it considers the following: (1) an application for an order for electronic surveillance under Title I of FISA; (2) an application for an order for access to business records under Title V of FISA; and (3) submissions from the government under Section 702 of FISA. As to applications for orders for access to business records under Title V of FISA, please describe whether the process for the Court's consideration of such applications is different when considering requests for bulk collection of phone call metadata records, as recently declassified by the Director of National Intelligence.*

Each week, one of the eleven district court judges who comprise the Court is on duty in Washington. As discussed below, most of the Court's work is handled by the duty judge with the assistance of attorneys and clerk's office personnel who staff the Court. Some of the Court's more complex or time-consuming matters are handled by judges outside of the duty-week system, at the discretion of the Presiding Judge. In either case, matters before the Court are thoroughly reviewed and analyzed by the Court.

Rule 9(a) of the United States Foreign Intelligence Surveillance Court Rules of Procedure

(FISC Rules of Procedure)<sup>1</sup> requires that except in certain circumstances (i.e., a submission pursuant to an emergency authorization under the statute or as otherwise permitted by the Court), a proposed application must be submitted by the government no later than seven days before the government seeks to have the matter entertained.<sup>2</sup> Upon the Court's receipt of a proposed application for an order under FISA, a member of the Court's legal staff reviews the application and evaluates whether it meets the legal requirements under the statute. As part of this evaluation, a Court attorney will often have one or more telephone conversations with the government<sup>3</sup> to seek additional information and/or raise concerns about the application. A Court attorney then prepares a written analysis of the application for the duty judge, which includes an identification of any weaknesses, flaws, or other concerns. For example, the attorney may recommend that the judge consider requiring the addition of information to the application; imposing special reporting requirements;<sup>4</sup> or shortening the requested duration of an authorization.

The judge then reviews the proposed application, as well as the attorney's written analysis.<sup>5</sup> The judge typically makes a preliminary determination at that time about what course

---

<sup>1</sup> A copy of the FISC Rules of Procedure is appended hereto as Attachment A. The rules are also available at <http://www.uscourts.gov/uscourts/rules/FISC2010.pdf>.

<sup>2</sup> A proposed application is also sometimes referred to as a "read copy" and has been referred to in this manner in at least one recent congressional hearing. A proposed application or "read copy" is a near-final version of the government's application, which does not include the signatures of executive branch officials required by statutory provisions such as 50 U.S.C. §§ 1804(a)(6) and 1823(a)(6). As described below, in most circumstances, the government will subsequently file a final copy of an application pursuant to Rule 9(b) of the FISC Rules of Procedure. Both the proposed and final applications include proposed orders.

The process of using proposed applications and final applications is altogether similar to the process employed by other federal courts in considering applications for wiretap orders under Title III of the Omnibus Crime Control and Safe Streets Act of 1968, as amended ("Title III"), which is codified at 18 U.S.C. §§ 2510-2522.

<sup>3</sup> In discussing Court interactions with "the government" throughout this document, I am referring to interactions with attorneys in the Office of Intelligence of the National Security Division of the United States Department of Justice.

<sup>4</sup> Pursuant to 50 U.S.C. §§ 1805(d)(3) and 1824(d)(3), the Court is authorized to assess compliance with the statutorily-required minimization procedures by reviewing the circumstances under which information concerning United States persons was acquired, retained, or disseminated.

<sup>5</sup> For each application, the Court retains the attorney's written analysis and the notes made by the judge, so that if the government later seeks to renew the authorization, the judge who considers the next

of action to take. These courses of action might include indicating to Court staff that he or she is prepared to approve the application without a hearing; indicating an inclination to impose conditions on the approval of the application; determining that additional information is needed about the application; or determining that a hearing would be appropriate before deciding whether to grant the application. A staff attorney will then relay the judge's inclination to the government, and the government will typically proceed by providing additional information, or by submitting a final application (sometimes with amendments, at the government's election) for the Court's ruling pursuant to Rule 9(b) of the FISC Rules of Procedure. In conjunction with its submission of a final application, the government has an opportunity to request a hearing, even if the judge did not otherwise intend to require one. The government might request a hearing, for example, to challenge conditions that the judge has indicated he or she would impose on the approval of an application. If the judge schedules a hearing, the judge decides whether to approve the application thereafter. Otherwise, the judge makes a determination based on the final written application submitted by the government. In approving an application, a judge will sometimes issue a Supplemental Order in addition to signing the government's proposed orders. Often, a Supplemental Order imposes some form of reporting requirement on the government.

If after receiving a final application, the judge is inclined to deny it, the Court will prepare a statement of reason(s) pursuant to 50 U.S.C. § 1803(a)(1). In some cases, the government may decide not to submit a final application, or to withdraw one that has been submitted, after learning that the judge does not intend to approve it. The annual statistics provided to Congress by the Attorney General pursuant to 50 U.S.C. §§ 1807 and 1862(b) – frequently cited to in press reports as a suggestion that the Court's approval rate of applications is over 99% – reflect only the number of *final* applications submitted to and acted on by the Court. These statistics do not reflect the fact that many applications are altered prior to final submission or even withheld from final submission entirely, often after an indication that a judge would not approve them.<sup>6</sup>

Most applications under Title V of FISA are handled pursuant to the process described above. However, applications under Title V of FISA for bulk collection of phone call metadata records are normally handled by the weekly duty judge using a process that is similar to the one described above, albeit more exacting. The government typically submits a proposed application of this type more than one week in advance. The attorney who reviews the application spends a

---

application has the benefit of the prior thoughts of the judge(s) and staff, and a written record of any problems with the case.

<sup>6</sup> Notably, the approval rate for Title III wiretap applications (see note 2 above) is higher than the approval rate for FISA applications, even using the Attorney General's FISA statistics as the baseline for comparison, as recent statistics show that from 2008 through 2012, only five of 13,593 Title III wiretap applications were requested but not authorized. See Administrative Office of the United States Courts, *Wiretap Report 2012*, Table 7 (available at <http://www.uscourts.gov/uscourts/statistics/wiretapreports/2012/Table7.pdf>).

greater amount of time reviewing and preparing a written analysis of such an application, in part because the Court has always required detailed information about the government's implementation of this authority. The judge likewise typically spends a greater amount of time than he or she normally spends on an individual application, carefully considering the extensive information provided by the government and determining whether to seek more information or hold a hearing before ruling on the application.

As described above, the majority of applications submitted to the Court are handled on a seven-day cycle, by a judge sitting on a weekly duty schedule. Applications that are novel or more complex are sometimes handled on a longer time-line, usually require additional briefing, and are assigned by the Presiding Judge based on judges' availability. Section 702 (i.e., 50 U.S.C. § 1881a) applications<sup>7</sup> would typically fall into this category.

Where the Court's process for handling Section 702 applications differs from the process described above, it is largely based on the statutory requirements of that section, which was enacted as part of the FISA Amendments Act of 2008 (FAA). Pursuant to 50 U.S.C. §§ 1881a(g)(1)(A) & (g)(2)(D)(i), prior to the implementation of an authorization under Section 702, the Attorney General and the Director of National Intelligence must provide the Court with a written certification containing certain statutorily required elements, and that certification must include an effective date for the authorization that is at least 30 days after the submission of the written certification to the Court.<sup>8</sup> Under 50 U.S.C. § 1881a(i)(B), the Court must review the certification, as well as the targeting and minimization procedures adopted in accordance with 50 U.S.C. §§ 1881a(d) & (e), not later than 30 days after the date on which the certification and procedures are submitted. The statutorily-imposed deadline for the Court's review typically coincides with the effective date identified in the final certification filed with the Court.

The government's submission of a Section 702 application typically includes a cover filing that highlights any special issues and identifies any changes that have been made relative to the prior application. The government has typically filed proposed (read copy) Section 702 applications approximately one month before filing a final application. Proposed Section 702 applications are reviewed by multiple members of the Court's legal staff. At the direction of the Presiding Judge or a judge who has been assigned to handle the Section 702 application, the

---

<sup>7</sup> "Section 702 application" is used here to refer collectively to a Section 702 certification and supporting affidavit, as well as to the statutorily-required targeting and minimization procedures.

<sup>8</sup> If the acquisition has already begun (e.g., pursuant to a determination of exigent circumstances under 50 U.S.C. § 1881a(c)(2)) or the effective date is less than 30 days after the submission of the written certification to the Court (e.g., because of an amendment to a certification while judicial review is pending, pursuant to 50 U.S.C. § 1881a(i)(1)(C)), 50 U.S.C. § 1881a(g)(2)(D)(ii) requires the certification to include the date the acquisition began or the effective date of the authorization.



Court's legal staff may request a meeting with the government to discuss a proposed application. Also at the direction of the Presiding Judge or a judge who has been assigned to handle the Section 702 application, the Court legal staff may request additional information from the government or convey a judge's concerns about the legal sufficiency of a proposed Section 702 application. Following these interactions, the government files a final Section 702 application, which the government may have elected to amend based on any concerns raised by the judge.

The judge reviews the final Section 702 application and may set a hearing if he or she has additional questions about it. If the judge finds (based on the written submission alone or the written submission in combination with a hearing) that the certification contains all of the required elements, and that the targeting and minimization procedures adopted in accordance with 50 U.S.C. §§ 1881a(d) & (e) are consistent with the requirements of those subsections and with the Fourth Amendment to the Constitution of the United States, the judge enters an order approving the certification in accordance with 50 U.S.C. § 1881a(i)(3)(A). As required by 50 U.S.C. § 1881a(i)(3)(C), the judge also issues an opinion in support of the order. If the judge finds that the certification does not contain the required elements or the targeting and minimization procedures are inconsistent with the requirements of 50 U.S.C. §§ 1881a(d) & (e), or the Fourth Amendment, the judge will, pursuant to 50 U.S.C. § 1881a(i)(3)(B), issue an order directing the government to, at the government's election and to the extent required by the Court's order, either correct any deficiency identified by the Court's order not later than 30 days after the date on which the Court issues the order, or cease, or not begin, the implementation of the authorization for which the certification was submitted. Subsequent review of any remedial measures taken by the government may then be required and may result in another order and opinion pursuant to 50 U.S.C. § 1881a(i).

2. *When considering such applications and submissions, please describe the interaction between the government and the Court (including both judges and court staff), including any hearings, meetings, or other means through which the Court has the opportunity to ask questions or seek additional information from the government. Please describe how frequently such exchanges occur, and generally what types of additional information that the Court might request of the government, if any. Please also describe how frequently the Court asks the government to make changes to its applications and submissions before ruling.*

The process through which the Court interacts with the government in reviewing proposed applications, seeking additional information, conveying Court concerns, and adjudicating final applications, is very similar to the process employed by other federal courts in considering applications for wiretap orders under Title III (discussed in notes 2 and 6 above).

Under FISA practice, the first set of interactions often take place at the staff level. The Court's legal staff frequently interacts with the government in various ways in the context of

examining the legal sufficiency of applications before they are presented in final form to a judge. Indeed, in the process of reviewing the government's applications and submissions in order to provide advice to the judge, the legal staff interact with the government on a daily basis. These daily interactions typically consist of secure telephone conversations in which legal staff ask the government questions about the legal and factual elements of applications or submissions. These questions may originate with legal staff after an initial review of an application or submission, or they may come from a judge.

At the direction of the Presiding Judge or the judge assigned to a matter, Court legal staff sometimes meet with the government in connection with applications and submissions. The Court typically requests such meetings when a proposed application or submission presents a special legal or factual concern about which the Court would like additional information (e.g., a novel use of technology or a request to use a new surveillance or search technique). The frequency of such meetings varies depending on the Court's assessment of its need for additional information in matters before it and the most conducive means to obtain that information. Court legal staff may meet with the government as often as 2-3 times a week, or as few as 1-2 times a month, in connection with the various matters pending before the Court.

Pursuant to 50 U.S.C. § 1803(a)(2)(A) and Rule 17(a) of the FISC Rules of Procedure, the Court also holds hearings in cases in which a judge assesses that he or she needs additional information in order to rule on a matter. The frequency of hearings varies depending on the nature and complexity of matters pending before the Court at a given time, and also, to some extent, based on the individual preferences of different judges. Hearings are attended, at a minimum, by the Department of Justice attorney who prepared the application and a fact witness from the agency seeking the Court's authorization.

The types of additional information sought from the government – through telephone conversations, meetings, or hearings – include, but are not limited to, the following: additional facts to justify the government's belief that its application meets the legal requirements for the type of authority it is seeking (e.g., in the case of electronic surveillance, that might include additional information to justify the government's belief that a target of surveillance is a foreign power or an agent of a foreign power, as required by 50 U.S.C. § 1804(a)(3)(A), or that the target is using or about to use a particular facility, as required by 50 U.S.C. § 1804(a)(3)(B)); additional facts about how the government intends to implement statutorily required minimization procedures (see, e.g., 50 U.S.C. §§ 1801(h); 1805(a)(3); 1824(a)(3); 1861(c)(1); 1881a(i)(3)(A); and 1881c(c)(1)(c)); additional information about the government's prior implementation of a Court order, particularly if the government has previously failed to comply fully with a Court order; or additional information about novel issues of technology or law (see Rule 11 of FISC Rules of Procedure).

In a typical week, the Court seeks additional information or modifies the terms proposed

by the government in a significant percentage of cases.<sup>9</sup> (The Court has recently initiated the process of tracking more precisely how frequently this occurs.) The judge may determine, for example, that he or she cannot make the necessary findings under the statute without the addition of information to the application, or that he or she can approve only some of the authorities sought through the application. The government then has the choice to alter its final application or proposed orders in response to the judge's concerns; request a hearing to address those concerns; submit a final application without changes; or elect not to proceed at all with a final application. If the government files a final application, the Court may, on its own, make changes to the government's proposed orders (or issue totally redrafted orders) to address the judge's concern about a given application. The judge may choose, for example, to make an authorization of a shorter duration than what was requested by the government, or the judge may issue a Supplemental Order imposing special reporting or minimization requirements on the government's implementation of an authorization.

3. *Public FISA Court opinions and orders make clear that the Court has considered the views of non-governmental parties in certain cases, including a provider challenge to the Protect America Act of 2007. Describe instances where non-governmental parties have appeared before the Court. Has the Court invited or heard views from a nongovernmental party regarding applications or submissions under Title I, Title V, or Title VII of FISA? If so, how did this come about, and what was the process or mechanism that the Court used to enable such views to be considered?*

FISA does not provide a mechanism for the Court to invite the views of nongovernmental parties. In fact, the Court's proceedings are *ex parte* as required by the statute (see, e.g., 50 U.S.C. §§ 1805(a), 1824(a), 1842(d)(1) & 1861(c)(1)), and in keeping with the procedures followed by other courts in applications for search warrants and wiretap orders. Nevertheless, the statute and the FISC Rules of Procedure provide multiple opportunities for recipients of Court orders or government directives to challenge those orders or directives, either directly or through refusal to comply with orders or directives. Additionally, as detailed below, there have been several instances – particularly in the past several months – in which nongovernmental parties have appeared before the Court outside of the context of a challenge to an individual Court order or government directive.

There has been one instance in which the Court heard arguments from a nongovernmental party that sought to substantively contest a directive from the government. Specifically, in 2007, the government issued directives to Yahoo!, Inc. (Yahoo) pursuant to Section 105B of the Protect America Act of 2007 (PAA). Yahoo refused to comply with the directives, and the government

---

<sup>9</sup> This assessment does not include minor technical or typographical changes, which occur more frequently.

filed a motion with this Court to compel compliance. The Court ordered and received briefing from both parties, and rendered a decision in April 2008.<sup>10</sup>

As noted above, the FISC Rules of Procedure and the FISA statute provide opportunities for the appearance of nongovernmental parties before the Court in matters pending pursuant to Titles I, V and VII of the statute. For example, Rule 19(a) of the FISC Rules of Procedure provides that if a person or entity served with a Court order fails to comply with that order, the government may file a motion for an order to show cause why the recipient should not be held in contempt and sanctioned accordingly. Thus, a nongovernmental party served with an order may invite an opportunity to be heard by the Court through refusal to comply with an order.

With respect to applications filed under Title V of FISA, 50 U.S.C. § 1861(f)(2)(A)(i) provides that a person receiving a production order may challenge the legality of that order by filing a petition with the Court. The same section of the statute provides that the recipient of a production order may challenge the non-disclosure order imposed in connection with a production order by filing a petition to modify or set aside the nondisclosure order. Rules 33-36 of the FISC Rules of Procedure delineate the procedures and requirements for filing such petitions, including the time limits on such challenges. To date, no recipient of a production order has opted to invoke this section of the statute.

With respect to applications filed under Title VII of FISA, 50 U.S.C. § 1881a(h)(4)(A) provides that an electronic communication service provider who receives a directive pursuant to Section 702 may file a petition to modify or set aside the directive with the Court. Sections 1881a(h)(4)(A)-(G) of the statute, as well as Rule 28 of the FISC Rules of Procedure, delineate

---

<sup>10</sup> Yahoo thereafter appealed the Court's decision to the Foreign Intelligence Surveillance Court of Review (FISCR). See *In re Directives [redacted] Pursuant to Section 105b of the Foreign Intelligence Surveillance Act*, 551 F.3d 1004 (FISA Ct. Rev. 2008). This is not the only instance in which a nongovernmental entity has appeared before the FISCR. In 2002, the FISCR accepted briefs filed by the ACLU and the National Association of Criminal Defense Lawyers as *amici curiae* in *In re Sealed Case*, 310 F.3d 717 (FISA Ct. Rev. 2002).

While Yahoo's identity as the provider that challenged these directives was previously under seal pursuant to the FISCR's decision in *In re Directives*, 551 F.3d 1004, 1016-18, the FISCR issued an Order on June 26, 2013, indicating that it does not object to the release of Yahoo's identity, and ordering, among other things, a new declassification review of the FISCR's opinion in *In re Directives*. The FISCR issued this order in response to a motion by Yahoo's counsel, and after receiving briefing by Yahoo and the government. Yahoo also recently filed a motion for publication of the Court's decision that was appealed to the FISCR, resulting in the published opinion in *In re Directives*. The Court granted the motion. Documents related to Yahoo's recent motion to this Court are available at <http://www.uscourts.gov/uscourts/courts/fisc/index.html> under Docket No. 105B(g) 07-01.

the procedures and requirements for such challenges. Relatedly, 50 U.S.C. § 1881a(h)(5)(A) provides that if an electronic communication service provider fails to comply with a directive issued under Section 702, the Attorney General may file a petition with the Court for an order to compel compliance, which would likely result in the service provider's appearance before the Court through its legal representatives. (Section 1881a(h)(5), as well as Rule 29 of the FISC Rules of Procedure, provide further detail on the procedures and requirements for the enforcement of Section 702 directives.) Finally, 50 U.S.C. § 1881a(h)(6) and Rule 31 of the FISC Rules of Procedure allow for the government or an electronic communication service provider to appeal an order of this Court under §§ 1881a(h)(4) or (5) to the FISCR. To date, no electronic communication service provider has opted to challenge a directive issued pursuant to Section 702, although, as noted above, Yahoo refused to comply with government directives issued under the PAA, which resulted in the government invoking a provision under that statute to compel compliance.

As noted above, there have been a number of other instances in which nongovernmental parties have appeared before the Court outside of the context of a direct challenge to a court order or a government directive, particularly recently. Those instances are as follows:

In August 2007, the American Civil Liberties Union (ACLU) filed a motion with the Court for the release of certain records. The Court ordered and received briefing on the matter from the ACLU and the government, and rendered a decision in December 2007. *See In re Motion for Release of Court Records*, 526 F. Supp. 2d 484 (FISA Ct. 2007).

On May 23, 2013, the Electronic Frontier Foundation (EFF) filed a motion with this Court for consent to disclosure of court records, or in the alternative, a determination of the effect of the Court's rules on access rights under the Freedom of Information Act. Following briefing by EFF and the government, the Court issued an Opinion and Order on June 12, 2013. All documents filed in this docket are available at <http://www.uscourts.gov/uscourts/courts/fisc/index.html> under Case No. Misc. 13-01.

On June 12, 2013, the ACLU, the American Civil Liberties Union of the Nation's Capital, and the Media Freedom and Information Access Clinic (Movants) filed a motion with this Court for the release of Court records. The Court ordered and has received briefing on the matter from the Movants and the government. On July 18, 2013, the Court granted the motions of (1) sixteen members of the House of Representatives and (2) a coalition of news media organizations for leave to file *amicus curiae* briefs in this case. The matter is pending before the Court. All documents filed in this docket are available at <http://www.uscourts.gov/uscourts/courts/fisc/index.html> under Case No. Misc. 13-02.

On June 18, 2013, Google, Inc. filed a motion with this Court for declaratory judgment of the company's first amendment right to publish aggregate information about FISA orders. The

court ordered briefing on the matter. On July 18, 2013, the Court granted the motions of (1) a coalition of news media organizations and (2) the First Amendment Coalition, the ACLU, the Center for Democracy and Technology, the EFF, and Techfreedom for leave to file *amicus curiae* briefs in this case. The matter is pending before the Court. All documents filed in this docket are available at <http://www.uscourts.gov/uscourts/courts/fisc/index.html> under Case No. Misc. 13-03.

On June 19, 2013, Microsoft Corporation filed a motion in this Court for declaratory judgment or other appropriate relief authorizing disclosure of aggregate data regarding any FISA orders it has received. The court ordered briefing on the matter. On July 18, 2013, the Court granted the motions of (1) a coalition of news media organizations and (2) the First Amendment Coalition, the ACLU, the Center for Democracy and Technology, the EFF, and Techfreedom for leave to file *amicus curiae* briefs in this case. The matter is pending before the Court. All documents filed in this docket are available at <http://www.uscourts.gov/uscourts/courts/fisc/index.html> under Case No. Misc. 13-04.

4. *Please describe the process used by the Court to consider and resolve any instances where the government notifies the Court of compliance concerns with any of the FISA authorities.*

Pursuant to 50 U.S.C. § 1803(h), the Court is empowered to ensure compliance with its orders. Additionally, Rule 13(a) of the FISC Rules of Procedure requires the government to file a written notice with the Court immediately upon discovering that any authority or approval granted by the Court has been implemented (either by government officials or others operating pursuant to Court order) in a manner that did not comply with the Court's authorization or approval or with applicable law. Rule 13(a) also requires the government to notify the Court in writing of the facts and circumstances relevant to the non-compliance; any modifications the government has made or proposes to make in how it will implement any authority or approval granted by the Court; and how the government proposes to dispose of or treat any information obtained as a result of the non-compliance.

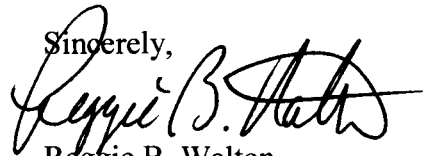
When the government discovers instances of non-compliance, it files notices with the Court as required by Rule 13(a). Because the rule requires the government to "immediately inform the Judge" of a compliance incident, the government typically files a preliminary notice that provides whatever facts are available at the time an incident is discovered. The legal staff review these notices as they are received and call significant matters to the attention of the appropriate judge. In instances in which the non-compliance has not been fully addressed by the time the preliminary Rule 13(a) notice is filed, the Court may seek additional information through telephone calls, meetings, or hearings. Typically, the government will file a final Rule 13(a) notice once the relevant facts are known and any unauthorized collection has been destroyed. However, judges sometimes issue orders directing the government to take specific

Honorable Patrick J. Leahy  
July 29, 2013  
Page 11

actions to address instances of non-compliance either before or after a final notice is filed, and, less frequently, to cease a course of action that the Court considers non-compliant. This process is followed for compliance issues in all matters, including matters handled under Title V and Section 702.

I hope these responses are helpful to the Senate Judiciary Committee in its deliberations.

Sincerely,

A handwritten signature in black ink, appearing to read "Reggie B. Walton". The signature is fluid and cursive, with a long horizontal stroke at the end.

Reggie B. Walton  
Presiding Judge

Identical letter sent to:           Honorable Charles E. Grassley

TO THE BENCH, BAR AND PUBLIC:

The attached *Rules of Procedure* for the Foreign Intelligence Surveillance Court supersede both the February 17, 2006 *Rules of Procedure* and the May 5, 2006 *Procedures for Review of Petitions Filed Pursuant to Section 501(f) of the Foreign Intelligence Surveillance Act of 1978, As Amended*. These revised *Rules of Procedure* are effective immediately.

John D. Bates  
Presiding Judge  
Foreign Intelligence Surveillance Court

November 1, 2010



**UNITED STATES FOREIGN  
INTELLIGENCE SURVEILLANCE COURT  
Washington, D.C.**

**RULES OF PROCEDURE  
*Effective November 1, 2010***

<b>Rule</b>	<b>Page</b>
<b>Title I. Scope of Rules; Amendment</b>	
1. Scope of Rules .....	1
2. Amendment .....	1
<b>Title II. National Security Information</b>	
3. National Security Information .....	1
<b>Title III. Structure and Powers of the Court</b>	
4. Structure .....	1
5. Authority of the Judges .....	1
<b>Title IV. Matters Presented to the Court</b>	
6. Means of Requesting Relief from the Court .....	2
7. Filing Applications, Certifications, Petitions, Motions, or Other Papers (“Submissions”) .....	2
8. Service .....	3
9. Time and Manner of Submission of Applications .....	3
10. Computation of Time .....	4
11. Notice and Briefing of Novel Issues .....	4
12. Submission of Targeting and Minimization Procedures .....	5
13. Correction of Misstatement or Omission; Disclosure of Non-Compliance .....	5
14. Motions to Amend Court Orders .....	5
15. Sequestration .....	5
16. Returns .....	6
<b>Title V. Hearings, Orders, and Enforcement</b>	
17. Hearings .....	6
18. Court Orders .....	6
19. Enforcement of Orders .....	7

**Title VI. Supplemental Procedures for Proceedings Under 50 U.S.C. § 1881a(h)**

20. Scope	7
21. Petition to Modify or Set Aside a Directive	7
22. Petition to Compel Compliance With a Directive	7
23. Contents of Petition	8
24. Response	8
25. Length of Petition and Response; Other Papers	8
26. Notification of Presiding Judge	8
27. Assignment	8
28. Review of Petition to Modify or Set Aside a Directive	9
29. Review of Petition to Compel Compliance Pursuant to 50 U.S.C. § 1881a(h)(5)(C)	9
30. <i>In Camera</i> Review	9
31. Appeal	9

**Title VII. Supplemental Procedures for Proceedings Under 50 U.S.C. § 1861(f)**

32. Scope	10
33. Petition Challenging Production or Nondisclosure Order	10
34. Contents of Petition	10
35. Length of Petition	10
36. Request to Stay Production	10
37. Notification of Presiding Judge	10
38. Assignment	11
39. Initial Review	11
40. Response to Petition; Other Papers	11
41. Rulings on Non-frivolous Petitions	11
42. Failure to Comply	12
43. <i>In Camera</i> Review	12
44. Appeal	12

**Title VIII. En Banc Proceedings**

45. Standard for Hearing or Rehearing En Banc	12
46. Initial Hearing En Banc on Request of a Party	12
47. Rehearing En Banc on Petition by a Party	12
48. Circulation of En Banc Petitions and Responses	13
49. Court-Initiated En Banc Proceedings	13
50. Polling	13
51. Stay Pending En Banc Review	13
52. Supplemental Briefing	13
53. Order Granting or Denying En Banc Review	13

**Title IX. Appeals**

54. How Taken ..... 14  
55. When Taken ..... 14  
56. Stay Pending Appeal ..... 14  
57. Motion to Transmit the Record ..... 14  
58. Transmitting the Record ..... 14  
59. Oral Notification to the Court of Review ..... 14

**Title X. Administrative Provisions**

60. Duties of the Clerk ..... 14  
61. Office Hours ..... 15  
62. Release of Court Records ..... 15  
63. Practice Before Court ..... 15

## **Title I. Scope of Rules; Amendment**

**Rule 1. Scope of Rules.** These rules, which are promulgated pursuant to 50 U.S.C. § 1803(g), govern all proceedings in the Foreign Intelligence Surveillance Court ("the Court"). Issues not addressed in these rules or the Foreign Intelligence Surveillance Act, as amended ("the Act"), may be resolved under the Federal Rules of Criminal Procedure or the Federal Rules of Civil Procedure.

**Rule 2. Amendment.** Any amendment to these rules must be promulgated in accordance with 28 U.S.C. § 2071.

## **Title II. National Security Information**

**Rule 3. National Security Information.** In all matters, the Court and its staff shall comply with the security measures established pursuant to 50 U.S.C. §§ 1803(c), 1822(e), 1861(f)(4), and 1881a(k)(1), as well as Executive Order 13526, "Classified National Security Information" (or its successor). Each member of the Court's staff must possess security clearances at a level commensurate to the individual's responsibilities.

## **Title III. Structure and Powers of the Court**

### **Rule 4. Structure.**

**(a) Composition.** In accordance with 50 U.S.C. § 1803(a), the Court consists of United States District Court Judges appointed by the Chief Justice of the United States.

**(b) Presiding Judge.** The Chief Justice designates the "Presiding Judge."

### **Rule 5. Authority of the Judges.**

**(a) Scope of Authority.** Each Judge may exercise the authority vested by the Act and such other authority as is consistent with Article III of the Constitution and other statutes and laws of the United States, to the extent not inconsistent with the Act.

**(b) Referring Matters to Other Judges.** Except for matters involving a denial of an application for an order, a Judge may refer any matter to another Judge of the Court with that Judge's consent. If a Judge directs the government to supplement an application, the Judge may direct the government to present the renewal of that application to the same Judge. If a matter is presented to a Judge who is unavailable or whose tenure on the Court expires while the matter is pending, the Presiding Judge may re-assign the matter.

**(c) Supplementation.** The Judge before whom a matter is pending may order a party to furnish any information that the Judge deems necessary.

## **Title IV. Matters Presented to the Court**

### **Rule 6. Means of Requesting Relief from the Court.**

- (a) Application.** The government may, in accordance with 50 U.S.C. §§ 1804, 1823, 1842, 1861, 1881b(b), 1881c(b), or 1881d(a), file an application for a Court order (“application”).
- (b) Certification.** The government may, in accordance with 50 U.S.C. § 1881a(g), file a certification concerning the targeting of non-United States persons reasonably believed to be located outside the United States (“certification”).
- (c) Petition.** A party may, in accordance with 50 U.S.C. §§ 1861(f) and 1881a(h) and the Supplemental Procedures in Titles VI and VII of these Rules, file a petition for review of a production or nondisclosure order issued under 50 U.S.C. § 1861 or for review or enforcement of a directive issued under 50 U.S.C. § 1881a (“petition”).
- (d) Motion.** A party seeking relief, other than pursuant to an application, certification, or petition permitted under the Act and these Rules, must do so by motion (“motion”).

### **Rule 7. Filing Applications, Certifications, Petitions, Motions, or Other Papers (“Submissions”).**

- (a) Filing.** A submission is filed by delivering it to the Clerk or as otherwise directed by the Clerk in accordance with Rule 7(k).
- (b) Original and One Copy.** Except as otherwise provided, a signed original and one copy must be filed with the Clerk.
- (c) Form.** Unless otherwise ordered, all submissions must be:
  - (1) on 8½-by-11-inch opaque white paper; and
  - (2) typed (double-spaced) or reproduced in a manner that produces a clear black image.
- (d) Electronic Filing.** The Clerk, when authorized by the Court, may accept and file submissions by any reliable, and appropriately secure, electronic means.
- (e) Facsimile or Scanned Signature.** The Clerk may accept for filing a submission bearing a facsimile or scanned signature in lieu of the original signature. Upon acceptance, a submission bearing a facsimile or scanned signature is the original Court record.
- (f) Citations.** Each submission must contain citations to pertinent provisions of the Act.
- (g) Contents.** Each application and certification filed by the government must be approved and certified in accordance with the Act, and must contain the statements and other information required by the Act.
- (h) Contact Information in Adversarial Proceedings.**
  - (1) Filing by a Party Other Than the Government.** A party other than the government must include in the initial submission the party’s full name, address, and telephone number, or, if the party is represented by counsel, the full name of the party and the party’s counsel, as well as counsel’s address, telephone number, facsimile number, and bar membership information.
  - (2) Filing by the Government.** In an adversarial proceeding, the initial

submission filed by the government must include the full names of the attorneys representing the United States and their mailing addresses, telephone numbers, and facsimile numbers.

**(i) Information Concerning Security Clearances in Adversarial Proceedings.** A party other than the government must:

- (1) state in the initial submission whether the party (or the party's responsible officers or employees) and counsel for the party hold security clearances;
- (2) describe the circumstances in which such clearances were granted; and
- (3) identify the federal agencies granting the clearances and the classification levels and compartments involved.

**(j) Ex Parte Review.** At the request of the government in an adversarial proceeding, the Judge must review *ex parte* and *in camera* any submissions by the government, or portions thereof, which may include classified information. Except as otherwise ordered, if the government files *ex parte* a submission that contains classified information, the government must file and serve on the non-governmental party an unclassified or redacted version. The unclassified or redacted version, at a minimum, must clearly articulate the government's legal arguments.

**(k) Instructions for Delivery to the Court.** A party may obtain instructions for making submissions permitted under the Act and these Rules by contacting the Clerk at (202) 357-6250.

#### **Rule 8. Service.**

**(a) By a Party Other than the Government.** A party other than the government must, at or before the time of filing a submission permitted under the Act and these Rules, serve a copy on the government. Instructions for effecting service must be obtained by contacting the Security and Emergency Planning Staff, United States Department of Justice, by telephone at (202) 514-2094.

**(b) By the Government.** At or before the time of filing a submission in an adversarial proceeding, the government must, subject to Rule 7(j), serve a copy by hand delivery or by overnight delivery on counsel for the other party, or, if the party is not represented by counsel, on the party directly.

**(c) Certificate of Service.** A party must include a certificate of service specifying the time and manner of service.

#### **Rule 9. Time and Manner of Submission of Applications.**

**(a) Proposed Applications.** Except when an application is being submitted following an emergency authorization pursuant to 50 U.S.C. §§ 1805(e), 1824(e), 1843, 1881b(d), or 1881c(d) ("emergency authorization"), or as otherwise permitted by the Court, proposed applications must be submitted by the government no later than seven days before the government seeks to have the matter entertained by the Court. Proposed applications submitted following an emergency authorization must be submitted as soon after such authorization as is reasonably practicable.

**(b) Final Applications.** Unless the Court permits otherwise, the final application,

including all signatures, approvals, and certifications required by the Act, must be filed no later than 10:00 a.m. Eastern Time on the day the government seeks to have the matter entertained by the Court.

**(c) Proposed Orders.** Each proposed application and final application submitted to the Court must include any pertinent proposed orders.

**(d) Number of Copies.** Notwithstanding Rule 7(b), unless the Court directs otherwise, only one copy of a proposed application must be submitted and only the original final application must be filed.

**(e) Notice of Changes.** No later than the time the final application is filed, the government must identify any differences between the final application and the proposed application.

**Rule 10. Computation of Time.** The following rules apply in computing a time period specified by these Rules or by Court order:

**(a) Day of the Event Excluded.** Exclude the day of the event that triggers the period.

**(b) Compute Time Using Calendar Days.** Compute time using calendar days, not business days.

**(c) Include the Last Day.** Include the last day of the period; but if the last day is a Saturday, Sunday, or legal holiday, the period continues to run until the next day that is not a Saturday, Sunday, or legal holiday.

**Rule 11. Notice and Briefing of Novel Issues.**

**(a) Notice to the Court.** If a submission by the government for Court action involves an issue not previously presented to the Court — including, but not limited to, a novel issue of technology or law — the government must inform the Court in writing of the nature and significance of that issue.

**(b) Submission Relating to New Techniques.** Prior to requesting authorization to use a new surveillance or search technique, the government must submit a memorandum to the Court that:

- (1) explains the technique;
- (2) describes the circumstances of the likely implementation of the technique;
- (3) discusses any legal issues apparently raised; and
- (4) describes the proposed minimization procedures to be applied.

At the latest, the memorandum must be submitted as part of the first proposed application or other submission that seeks to employ the new technique.

**(c) Novel Implementation.** When requesting authorization to use an existing surveillance or search technique in a novel context, the government must identify and address any new minimization or other issues in a written submission made, at the latest, as part of the application or other filing seeking such authorization.

**(d) Legal Memorandum.** If an application or other request for action raises an issue of law not previously considered by the Court, the government must file a memorandum of law in support of its position on each new issue. At the latest, the memorandum must be

submitted as part of the first proposed application or other submission that raises the issue.

**Rule 12. Submission of Targeting and Minimization Procedures.** In a matter involving Court review of targeting or minimization procedures, such procedures may be set out in full in the government's submission or may be incorporated by reference to procedures approved in a prior docket. Procedures that are incorporated by reference to a prior docket may be supplemented, but not otherwise modified, in the government's submission. Otherwise, proposed procedures must be set forth in a clear and self-contained manner, without resort to cross-referencing.

**Rule 13. Correction of Misstatement or Omission; Disclosure of Non-Compliance.**

**(a) Correction of Material Facts.** If 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;
- (4) any modifications the government has made or proposes to make in how it will implement any authority or approval granted by the Court; and
- (5) how the government proposes to dispose of or treat any information obtained as a result of the misstatement or omission.

**(b) Disclosure of Non-Compliance.** If the government discovers that any authority or approval granted by the Court has been implemented in a manner that did not comply with the Court's authorization or approval or with applicable law, the government, in writing, must immediately inform the Judge to whom the submission was made of:

- (1) the non-compliance;
- (2) the facts and circumstances relevant to the non-compliance;
- (3) any modifications the government has made or proposes to make in how it will implement any authority or approval granted by the Court; and
- (4) how the government proposes to dispose of or treat any information obtained as a result of the non-compliance.

**Rule 14. Motions to Amend Court Orders.** Unless the Judge who issued the order granting an application directs otherwise, a motion to amend the order may be presented to any other Judge.

**Rule 15. Sequestration.** Except as required by Court-approved minimization procedures, the government must not submit material for sequestration with the Court without the prior approval of the Presiding Judge. To obtain such approval, the government must, prior to tendering the material to the Court for sequestration, file a motion stating the circumstances of the material's acquisition and explaining why it is necessary for such material to be retained in the custody of the Court.



**Rule 16. Returns.**

**(a) Time for Filing.**

**(1) Search Orders.** Unless the Court directs otherwise, a return must be made and filed either at the time of submission of a proposed renewal application or within 90 days of the execution of a search order, whichever is sooner.

**(2) Other Orders.** The Court may direct the filing of other returns at a time and in a manner that it deems appropriate.

**(b) Contents.** The return must:

**(1)** notify the Court of the execution of the order;

**(2)** describe the circumstances and results of the search or other activity including, where appropriate, an inventory;

**(3)** certify that the execution was in conformity with the order or describe and explain any deviation from the order; and

**(4)** include any other information as the Court may direct.

**Title V. Hearings, Orders, and Enforcement**

**Rule 17. Hearings.**

**(a) Scheduling.** The Judge to whom a matter is presented or assigned must determine whether a hearing is necessary and, if so, set the time and place of the hearing.

**(b) Ex Parte.** Except as the Court otherwise directs or the Rules otherwise provide, a hearing in a non-adversarial matter must be *ex parte* and conducted within the Court's secure facility.

**(c) Appearances.** Unless excused, the government official providing the factual information in an application or certification and an attorney for the applicant must attend the hearing, along with other representatives of the government, and any other party, as the Court may direct or permit.

**(d) Testimony; Oath; Recording of Proceedings.** A Judge may take testimony under oath and receive other evidence. The testimony may be recorded electronically or as the Judge may otherwise direct, consistent with the security measures referenced in Rule 3.

**Rule 18. Court Orders.**

**(a) Citations.** All orders must contain citations to pertinent provisions of the Act.

**(b) Denying Applications.**

**(1) Written Statement of Reasons.** If a Judge denies the government's application, the Judge must immediately provide a written statement of each reason for the decision and cause a copy of the statement to be served on the government.

**(2) Previously Denied Application.** If a Judge denies an application or other request for relief by the government, any subsequent submission on the matter must be referred to that Judge.

**(c) Expiration Dates.** An expiration date in an order must be stated using Eastern Time and must be computed from the date and time of the Court's issuance of the order, or, if applicable, of an emergency authorization.

**(d) Electronic Signatures.** The Judge may sign an order by any reliable, appropriately secure electronic means, including facsimile.

**Rule 19. Enforcement of Orders.**

**(a) Show Cause Motions.** If a person or entity served with a Court order (the "recipient") fails to comply with that order, the government may file a motion for an order to show cause why the recipient should not be held in contempt and sanctioned accordingly. The motion must be presented to the Judge who entered the underlying order.

**(b) Proceedings.**

**(1)** An order to show cause must:

**(i)** confirm that the underlying order was issued;

**(ii)** schedule further proceedings; and

**(iii)** afford the recipient an opportunity to show cause why the recipient should not be held in contempt.

**(2)** A Judge must conduct any proceeding on a motion to show cause *in camera*. The Clerk must maintain all records of the proceedings in conformance with 50 U.S.C. § 1803(c).

**(3)** If the recipient fails to show cause for noncompliance with the underlying order, the Court may find the recipient in contempt and enter any order it deems necessary and appropriate to compel compliance and to sanction the recipient for noncompliance with the underlying order.

**(4)** If the recipient shows cause for noncompliance or if the Court concludes that the order should not be enforced as issued, the Court may enter any order it deems appropriate.

**Title VI. Supplemental Procedures for Proceedings Under 50 U.S.C. § 1881a(h)**

**Rule 20. Scope.** Together with the generally-applicable provisions of these Rules concerning filing, service, and other matters, these supplemental procedures apply in proceedings under 50 U.S.C. § 1881a(h).

**Rule 21. Petition to Modify or Set Aside a Directive.** An electronic communication service provider ("provider"), who receives a directive issued under 50 U.S.C. § 1881a(h)(1), may file a petition to modify or set aside such directive under 50 U.S.C. § 1881a(h)(4). A petition may be filed by the provider's counsel.

**Rule 22. Petition to Compel Compliance With a Directive.** In the event a provider fails to comply with a directive issued under 50 U.S.C. § 1881a(h)(1), the government may, pursuant to 50 U.S.C. § 1881a(h)(5), file a petition to compel compliance with the directive.

**Rule 23. Contents of Petition.** The petition must:

- (a) state clearly the relief being sought;
- (b) state concisely the factual and legal grounds for modifying, setting aside, or compelling compliance with the directive at issue;
- (c) include a copy of the directive and state the date on which the directive was served on the provider; and
- (d) state whether a hearing is requested.

**Rule 24. Response.**

- (a) **By Government.** The government may, within seven days following notification under Rule 28(b) that plenary review is necessary, file a response to a provider's petition.
- (b) **By Provider.** The provider may, within seven days after service of a petition by the government to compel compliance, file a response to the petition.

**Rule 25. Length of Petition and Response; Other Papers.**

- (a) **Length.** Unless the Court directs otherwise, a petition and response each must not exceed 20 pages in length, including any attachments (other than a copy of the directive at issue).
- (b) **Other papers.** No supplements, replies, or sur-replies may be filed without leave of the Court.

**Rule 26. Notification of Presiding Judge.** Upon receipt, the Clerk must notify the Presiding Judge that a petition to modify, set aside, or compel compliance with a directive issued under 50 U.S.C. § 1881a(h)(1) has been filed. If the Presiding Judge is not reasonably available when the Clerk receives a petition, the Clerk must notify each of the local Judges, in order of seniority on the Court, and, if necessary, each of the other Judges, in order of seniority on the Court, until a Judge who is reasonably available has received notification. The reasonably available Judge who receives notification will be the acting Presiding Judge ("Presiding Judge") for the case.

**Rule 27. Assignment.**

- (a) **Presiding Judge.** As soon as possible after receiving notification from the Clerk that a petition has been filed, and no later than 24 hours after the filing of the petition, the Presiding Judge must assign the matter to a Judge in the petition review pool established by 50 U.S.C. § 1803(e)(1). The Clerk must record the date and time of the assignment.
- (b) **Transmitting Petition.** The Clerk must transmit the petition to the assigned Judge as soon as possible but no later than 24 hours after being notified of the assignment by the Presiding Judge.

**Rule 28. Review of Petition to Modify or Set Aside a Directive.**

**(a) Initial Review Pursuant to 50 U.S.C. § 1881a(h)(4)(D).**

(1) A Judge must conduct an initial review of a petition to modify or set aside a directive within five days after being assigned such petition.

(2) If the Judge determines that the provider's claims, defenses, or other legal contentions are not warranted by existing law or by a nonfrivolous argument for extending, modifying, or reversing existing law or for establishing new law, the Judge must promptly deny such petition, affirm the directive, and order the provider to comply with the directive. Upon making such determination or promptly thereafter, the Judge must provide a written statement of reasons. The Clerk must transmit the ruling and statement of reasons to the provider and the government.

**(b) Plenary Review Pursuant to 50 U.S.C. § 1881a(h)(4)(E).**

(1) If the Judge determines that the petition requires plenary review, the Court must promptly notify the parties. The Judge must provide a written statement of reasons for the determination.

(2) The Judge must affirm, modify, or set aside the directive that is the subject of the petition within the time permitted under 50 U.S.C. §§ 1881a(h)(4)(E) and 1881a(j)(2).

(3) The Judge may hold a hearing or conduct proceedings solely on the papers filed by the provider and the government.

**(c) Burden.** Pursuant to 50 U.S.C. § 1881a(h)(4)(C), a Judge may grant the petition only if the Judge finds that the challenged directive does not meet the requirements of 50 U.S.C. § 1881a or is otherwise unlawful.

**(d) Continued Effect.** Pursuant to 50 U.S.C. § 1881a(h)(4)(F), any directive not explicitly modified or set aside by the Judge remains in full effect.

**Rule 29. Review of Petition to Compel Compliance Pursuant to 50 U.S.C. § 1881a(h)(5)(C).**

(a) The Judge reviewing the government's petition to compel compliance with a directive must, within the time permitted under 50 U.S.C. §§ 1881a(h)(5)(C) and 1881a(j)(2), issue an order requiring the provider to comply with the directive or any part of it, as issued or as modified, if the Judge finds that the directive meets the requirements of 50 U.S.C. § 1881a and is otherwise lawful.

(b) The Judge must provide a written statement of reasons for the determination. The Clerk must transmit the ruling and statement of reasons to the provider and the government.

**Rule 30. *In Camera* Review.** Pursuant to 50 U.S.C. § 1803(e)(2), the Court must review a petition under 50 U.S.C. § 1881a(h) and conduct related proceedings *in camera*.

**Rule 31. Appeal.** Pursuant to 50 U.S.C. § 1881a(h)(6) and subject to Rules 54 through 59 of these Rules, the government or the provider may petition the Foreign Intelligence Surveillance Court of Review ("Court of Review") to review the Judge's ruling.

**Title VII. Supplemental Procedures for Proceedings Under 50 U.S.C. § 1861(f)**

**Rule 32. Scope.** Together with the generally-applicable provisions of these Rules regarding filing, service, and other matters, these supplemental procedures apply in proceedings under 50 U.S.C. § 1861(f).

**Rule 33. Petition Challenging Production or Nondisclosure Order.**

**(a) Who May File.** The recipient of a production order or nondisclosure order under 50 U.S.C. § 1861 (“petitioner”) may file a petition challenging the order pursuant to 50 U.S.C. § 1861(f). A petition may be filed by the petitioner’s counsel.

**(b) Time to File Petition.**

**(1) Challenging a Production Order.** The petitioner must file a petition challenging a production order within 20 days after the order has been served.

**(2) Challenging a Nondisclosure Order.** A petitioner may not file a petition challenging a nondisclosure order issued under 50 U.S.C. § 1861(d) earlier than one year after the order was entered.

**(3) Subsequent Petition Challenging a Nondisclosure Order.** If a Judge denies a petition to modify or set aside a nondisclosure order, the petitioner may not file a subsequent petition challenging the same nondisclosure order earlier than one year after the date of the denial.

**Rule 34. Contents of Petition.** A petition must:

**(a)** state clearly the relief being sought;

**(b)** state concisely the factual and legal grounds for modifying or setting aside the challenged order;

**(c)** include a copy of the challenged order and state the date on which it was served on the petitioner; and

**(d)** state whether a hearing is requested.

**Rule 35. Length of Petition.** Unless the Court directs otherwise, a petition may not exceed 20 pages in length, including any attachments (other than a copy of the challenged order).

**Rule 36. Request to Stay Production.**

**(a) Petition Does Not Automatically Effect a Stay.** A petition does not automatically stay the underlying order. A production order will be stayed only if the petitioner requests a stay and the Judge grants such relief.

**(b) Stay May Be Requested Prior to Filing of a Petition.** A petitioner may request the Court to stay the production order before filing a petition challenging the order.

**Rule 37. Notification of Presiding Judge.** Upon receipt, the Clerk must notify the Presiding Judge that a petition challenging a production or nondisclosure order has been filed. If the Presiding Judge is not reasonably available when the Clerk receives the petition, the Clerk must

notify each of the local Judges, in order of seniority on the Court, and, if necessary, each of the other Judges, in order of seniority on the Court, until a Judge who is reasonably available has received notification. The reasonably available Judge who receives notification will be the acting Presiding Judge ("Presiding Judge") for the case.

**Rule 38. Assignment.**

**(a) Presiding Judge.** Immediately after receiving notification from the Clerk that a petition has been filed, the Presiding Judge must assign the matter to a Judge in the petition pool established by 50 U.S.C. § 1803(e)(1). The Clerk must record the date and time of the assignment.

**(b) Transmitting Petition.** The Clerk must transmit the petition to the assigned Judge as soon as possible but no later than 24 hours after being notified of the assignment by the Presiding Judge.

**Rule 39. Initial Review.**

**(a) When.** The Judge must review the petition within 72 hours after being assigned the petition.

**(b) Frivolous Petition.** If the Judge determines that the petition is frivolous, the Judge must:

- (1) immediately deny the petition and affirm the challenged order;
- (2) promptly provide a written statement of the reasons for the denial; and
- (3) provide a written ruling, together with the statement of reasons, to the Clerk, who must transmit the ruling and statement of reasons to the petitioner and the government.

**(c) Non-Frivolous Petition.**

**(1) Scheduling.** If the Judge determines that the petition is not frivolous, the Judge must promptly issue an order that sets a schedule for its consideration. The Clerk must transmit the order to the petitioner and the government.

**(2) Manner of Proceeding.** The judge may hold a hearing or conduct the proceedings solely on the papers filed by the petitioner and the government.

**Rule 40. Response to Petition; Other Papers.**

**(a) Government's Response.** Unless the Judge orders otherwise, the government must file a response within 20 days after the issuance of the initial scheduling order pursuant to Rule 39(c). The response must not exceed 20 pages in length, including any attachments (other than a copy of the challenged order).

**(b) Other Papers.** No supplements, replies, or sur-replies may be filed without leave of the Court.

**Rule 41. Rulings on Non-frivolous Petitions.**

**(a) Written Statement of Reasons.** If the Judge determines that the petition is not frivolous, the Judge must promptly provide a written statement of the reasons for modifying, setting aside, or affirming the production or nondisclosure order.

**(b) Affirming the Order.** If the Judge does not modify or set aside the production or nondisclosure order, the Judge must affirm it and order the recipient promptly to comply with it.

**(c) Transmitting the Judge's Ruling.** The Clerk must transmit the Judge's ruling and written statement of reasons to the petitioner and the government.

**Rule 42. Failure to Comply.** If a recipient fails to comply with an order affirmed under 50 U.S.C. § 1861(f), the government may file a motion seeking immediate enforcement of the affirmed order. The Court may consider the government's motion without receiving additional submissions or convening further proceedings on the matter.

**Rule 43. In Camera Review.** Pursuant to 50 U.S.C. § 1803(e)(2), the Court must review a petition under 50 U.S.C. § 1861(f) and conduct related proceedings *in camera*.

**Rule 44. Appeal.** Pursuant to 50 U.S.C. § 1861(f)(3) and subject to Rules 54 through 59 of these Rules, the government or the petitioner may petition the Court of Review to review the Judge's ruling.

### **Title VIII. En Banc Proceedings**

**Rule 45. Standard for Hearing or Rehearing En Banc.** Pursuant to 50 U.S.C. § 1803(a)(2)(A), the Court may order a hearing or rehearing en banc only if it is necessary to secure or maintain uniformity of the Court's decisions, or the proceeding involves a question of exceptional importance.

**Rule 46. Initial Hearing En Banc on Request of a Party.** The government in any proceeding, or a party in a proceeding under 50 U.S.C. § 1861(f) or 50 U.S.C. § 1881a(h)(4)-(5), may request that the matter be entertained from the outset by the full Court. However, initial hearings en banc are extraordinary and will be ordered only when a majority of the Judges determines that a matter is of such immediate and extraordinary importance that initial consideration by the en banc Court is necessary, and en banc review is feasible in light of applicable time constraints on Court action.

**Rule 47. Rehearing En Banc on Petition by a Party.**

**(a) Timing of Petition and Response.** A party may file a petition for rehearing en banc permitted under 50 U.S.C. § 1803(a)(2) no later than 30 days after the challenged order or decision is entered. In an adversarial proceeding in which a petition for rehearing en banc is permitted under § 1803(a)(2), a party must file a response to the petition within 14 days after filing and service of the petition.

**(b) Length of Petition and Response.** Unless the Court directs otherwise, a petition for rehearing en banc and a response to a petition for rehearing en banc each must not exceed 15 pages, including any attachments (other than the challenged order or decision).

**Rule 48. Circulation of En Banc Petitions and Responses.** The Clerk must, after consulting with the Presiding Judge and in a manner consistent with applicable security requirements, promptly provide a copy of any timely-filed en banc petition permitted under 50 U.S.C. § 1803(a)(2), and any timely-filed response thereto, to each Judge.

**Rule 49. Court-Initiated En Banc Proceedings.** A Judge to whom a matter has been presented may request that all Judges be polled with respect to whether the matter should be considered or reconsidered en banc. On a Judge's request, the Clerk must, after consulting with the Presiding Judge and in a manner consistent with applicable security requirements, promptly provide notice of the request, along with a copy of pertinent materials, to every Judge.

**Rule 50. Polling.**

**(a) Deadline for Vote.** The Presiding Judge must set a deadline for the Judges to submit their vote to the Clerk on whether to grant a hearing or rehearing en banc. The deadline must be communicated to all Judges at the time the petition or polling request is circulated.

**(b) Vote on Stay.** In the case of rehearing en banc, the Presiding Judge may request that all Judges also vote on whether and to what extent the challenged order or ruling should be stayed or remain in effect if rehearing en banc is granted, pending a decision by the en banc Court on the merits.

**Rule 51. Stay Pending En Banc Review.**

**(a) Stay or Modifying Order.** In accordance with 50 U.S.C. §§ 1803(a)(2)(B) and 1803(f), the Court en banc may enter a stay or modifying order while en banc proceedings are pending.

**(b) Statement of Position Regarding Continued Effect of Challenged Order.** A petition for rehearing en banc and any response to the petition each must include a statement of the party's position as to whether and to what extent the challenged order should remain in effect if rehearing en banc is granted, pending a decision by the en banc Court on the merits.

**Rule 52. Supplemental Briefing.** Upon ordering hearing or rehearing en banc, the Court may require the submission of supplemental briefs.

**Rule 53. Order Granting or Denying En Banc Review.**

**(a) Entry of Order.** If a majority of the Judges votes within the time allotted for polling that a matter be considered en banc, the Presiding Judge must direct the Clerk to enter an order granting en banc review. If a majority of the Judges does not vote to grant hearing or rehearing en banc within the time allotted for polling, the Presiding Judge must direct the Clerk to enter an order denying en banc review.

**(b) Other Issues.** The Presiding Judge may set the time of an en banc hearing and the time and scope of any supplemental hearing in the order granting en banc review. The



order may also address whether and to what extent the challenged order or ruling will be stayed or remain in effect pending a decision by the en banc Court on the merits.

### **Title IX. Appeals**

**Rule 54. How Taken.** An appeal to the Court of Review, as permitted by law, may be taken by filing a petition for review with the Clerk.

**Rule 55. When Taken.**

**(a) Generally.** Except as the Act provides otherwise, a party must file a petition for review no later than 30 days after entry of the decision or order as to which review is sought.

**(b) Effect of En Banc Proceedings.** Following the timely submission of a petition for rehearing en banc permitted under 50 U.S.C. § 1803(a)(2) or the grant of rehearing en banc on the Court's own initiative, the time otherwise allowed for taking an appeal runs from the date on which such petition is denied or dismissed or, if en banc review is granted, from the date of the decision of the en banc Court on the merits.

**Rule 56. Stay Pending Appeal.** In accordance with 50 U.S.C. § 1803(f), the Court may enter a stay of an order or an order modifying an order while an appeal is pending.

**Rule 57. Motion to Transmit the Record.** Together with the petition for review, the party filing the appeal must also file a motion to transmit the record to the Court of Review.

**Rule 58. Transmitting the Record.** The Clerk must arrange to transmit the record under seal to the Court of Review as expeditiously as possible, no later than 30 days after an appeal has been filed. The Clerk must include a copy of the Court's statement of reasons for the decision or order appealed from as part of the record on appeal.

**Rule 59. Oral Notification to the Court of Review.** The Clerk must orally notify the Presiding Judge of the Court of Review promptly upon the filing of a petition for review.

### **Title X. Administrative Provisions**

**Rule 60. Duties of the Clerk.**

**(a) General Duties.** The Clerk supports the work of the Court consistent with the directives of the Presiding Judge. The Presiding Judge may authorize the Clerk to delegate duties to staff in the Clerk's office or other designated individuals.

**(b) Maintenance of Court Records.** The Clerk:

**(1)** maintains the Court's docket and records — including records and recordings of proceedings before the Court — and the seal of the Court;

- (2) accepts papers for filing;
- (3) keeps all records, pleadings, and files in a secure location, making those materials available only to persons authorized to have access to them; and
- (4) performs any other duties, consistent with the usual powers of a Clerk of Court, as the Presiding Judge may authorize.

**Rule 61. Office Hours.** Although the Court is always open, the regular business hours of the Clerk's Office are 9:00 a.m. to 5:00 p.m. daily except Saturdays, Sundays, and legal holidays. Except when the government submits an application following an emergency authorization, or when the Court otherwise directs, any filing outside these hours will be recorded as received at the start of the next business day.

**Rule 62. Release of Court Records.**

(a) **Publication of Opinions.** The Judge who authored an order, opinion, or other decision may *sua sponte* or on motion by a party request that it be published. Upon such request, the Presiding Judge, after consulting with other Judges of the Court, may direct that an order, opinion or other decision be published. Before publication, the Court may, as appropriate, direct the Executive Branch to review the order, opinion, or other decision and redact it as necessary to ensure that properly classified information is appropriately protected pursuant to Executive Order 13526 (or its successor).

(b) **Other Records.** Except when an order, opinion, or other decision is published or provided to a party upon issuance, the Clerk may not release it, or other related record, without a Court order. Such records must be released in conformance with the security measures referenced in Rule 3.

(c) **Provision of Court Records to Congress.**

(1) **By the Government.** The government may provide copies of Court orders, opinions, decisions, or other Court records, to Congress, pursuant to 50 U.S.C. §§ 1871(a)(5), 1871(c), or 1881f(b)(1)(D), or any other statutory requirement, without prior motion to and order by the Court. The government, however, must contemporaneously notify the Court in writing whenever it provides copies of Court records to Congress and must include in the notice a list of the documents provided.

(2) **By the Court.** The Presiding Judge may provide copies of Court orders, opinions, decisions, or other Court records to Congress. Such disclosures must be made in conformance with the security measures referenced in Rule 3.

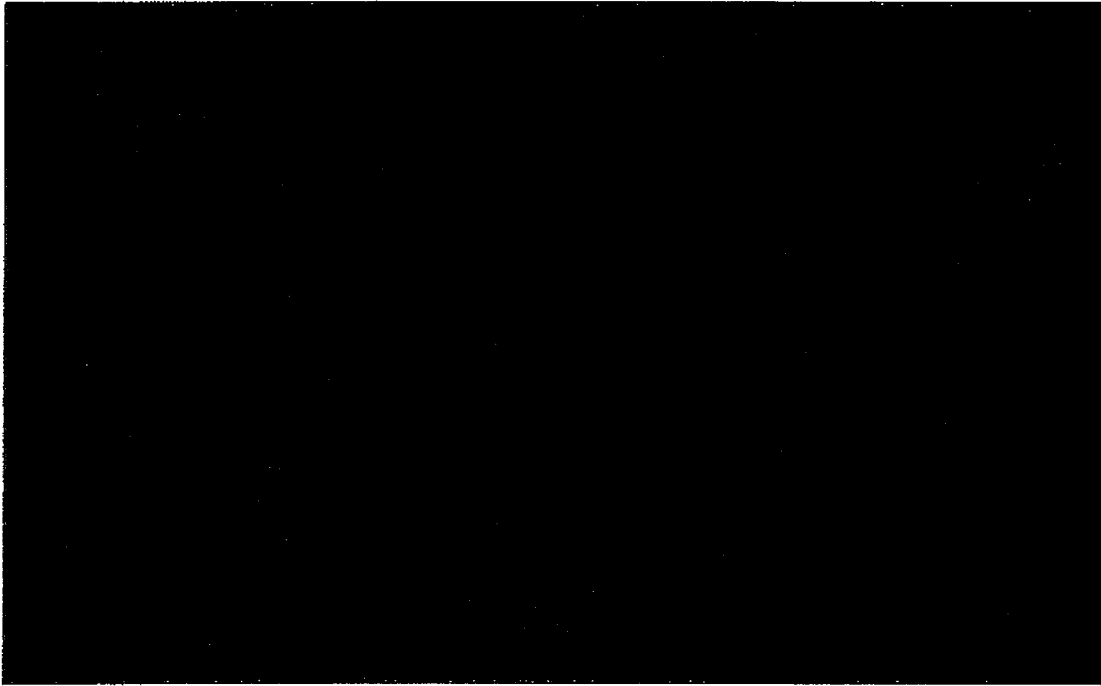
**Rule 63. Practice Before Court.** An attorney may appear on a matter with the permission of the Judge before whom the matter is pending. An attorney who appears before the Court must be a licensed attorney and a member, in good standing, of the bar of a United States district or circuit court, except that an attorney who is employed by and represents the United States or any of its agencies in a matter before the Court may appear before the Court regardless of federal bar membership. All attorneys appearing before the Court must have the appropriate security clearance.

# Exhibit 19

# Exhibit 20

~~TOP SECRET//COMINT//ORCON,NOFORN~~

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



**MEMORANDUM OPINION**

These matters are before the Foreign Intelligence Surveillance Court ("FISC" or "Court") on: (1) the "Government's Ex Parte Submission of Reauthorization Certification and Related Procedures, Ex Parte Submission of Amended Certifications, and Request for an Order Approving Such Certification and Amended Certifications" for DNI/AG 702(g) Certifications

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

[REDACTED], which was filed on April 20, 2011; (2) the “Government’s Ex Parte Submission of Reauthorization Certification and Related Procedures, Ex Parte Submission of Amended Certifications, and Request for an Order Approving Such Certification and Amended Certifications” for DNI/AG 702(g) Certifications [REDACTED], which was filed on April 22, 2011; and (3) the “Government’s Ex Parte Submission of Reauthorization Certification and Related Procedures, Ex Parte Submission of Amended Certifications, and Request for an Order Approving Such Certification and Amended Certifications” for DNI/AG 702(g) Certifications [REDACTED], which was also filed on April 22, 2011.<sup>1</sup>

Through these submissions, the government seeks approval of the acquisition of certain telephone and Internet communications pursuant to Section 702 of the Foreign Intelligence Surveillance Act (“FISA” or the “Act”), 50 U.S.C. § 1881a, which requires judicial review for compliance with both statutory and constitutional requirements. For the reasons set forth below, the government’s requests for approval are granted in part and denied in part. The Court concludes that one aspect of the proposed collection – the “upstream collection” of Internet transactions containing multiple communications – is, in some respects, deficient on statutory and constitutional grounds.

---

<sup>1</sup> For ease of reference, the Court will refer to these three filings collectively as the “April 2011 Submissions.”

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

I. BACKGROUND

A. The Certifications and Amendments

The April 2011 Submissions include DNI/AG 702(g) Certification [REDACTED]

[REDACTED], all of which were executed by the Attorney General and the Director of National Intelligence ("DNI") pursuant to Section 702. [REDACTED] previous certifications have been submitted by the government and approved by the Court pursuant to Section 702. [REDACTED]

[REDACTED] (collectively, the "Prior 702 Dockets"). Each of the April 2011 Submissions also includes supporting affidavits by the Director or Acting Director of the National Security Agency ("NSA"), the Director of the Federal Bureau of Investigation ("FBI"), [REDACTED] two sets of targeting procedures, for use by NSA and FBI respectively; and three sets of minimization procedures, for use by NSA, FBI, and CIA, respectively.<sup>2</sup>

Like the acquisitions approved by the Court in the eight Prior 702 Dockets, collection

---

<sup>2</sup> The targeting and minimization procedures accompanying Certification [REDACTED] are identical to those accompanying [REDACTED]. As discussed below, the NSA targeting procedures and FBI minimization procedures accompanying Certifications [REDACTED] also are identical to the NSA targeting procedures and FBI minimization procedures that were submitted by the government and approved by the Court for use in connection with Certifications [REDACTED]. The FBI targeting procedures and the NSA and CIA minimization procedures that accompany the April 2011 Submissions differ in several respects from the corresponding procedures that were submitted by the government and approved by the Court in connection with Certifications [REDACTED].

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

under Certifications [REDACTED] is limited to “the targeting of non-United States persons reasonably believed to be located outside the United States.” Certification [REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]

The April 2011 Submissions also include amendments to certifications that have been submitted by the government and approved by the Court in the Prior 702 Dockets. The amendments, which have been authorized by the Attorney General and the DNI, provide that information collected under the certifications in the Prior 702 Dockets will, effective upon the Court’s approval of Certifications [REDACTED], be handled subject to the same

~~TOP SECRET//COMINT//ORCON,NOFORN~~



~~TOP SECRET//COMINT//ORCON,NOFORN~~

revised NSA and CIA minimization procedures that have been submitted for use in connection with Certifications [REDACTED]

B. The May 2 "Clarification" Letter

On May 2, 2011, the government filed with the Court a letter pursuant to FISC Rule 13(a) titled "Clarification of National Security Agency's Upstream Collection Pursuant to Section 702 of FISA" ("May 2 Letter"). The May 2 Letter disclosed to the Court for the first time that NSA's "upstream collection"<sup>3</sup> of Internet communications includes the acquisition of entire "transaction[s]" [REDACTED]

[REDACTED]<sup>4</sup> According to the May 2 Letter, such transactions may contain data that is wholly unrelated to the tasked selector, including the full content of discrete communications that are not to, from, or about the facility tasked for collection. See id., at 2-3. The letter noted that NSA uses [REDACTED] to ensure that "the person from whom it seeks to obtain foreign intelligence information is located overseas," but suggested that the government might lack confidence in the effectiveness of such measures as applied to Internet transactions. See id., at 3 (citation omitted).

---

<sup>3</sup> The term "upstream collection" refers to NSA's interception of Internet communications as they transit [REDACTED], rather than to acquisitions directly from Internet service providers such as [REDACTED].

<sup>4</sup> The concept of "Internet transactions" is discussed more fully below. See infra, pages 27-41 and note 23.

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

C. The Government's First Motion for Extensions of Time

On May 5, 2011, the government filed a motion seeking to extend until July 22, 2011, the 30-day periods in which the Court must otherwise complete its review of Certifications [REDACTED], and the amendments to the certifications in the Prior 702 Dockets. See Motion for an Order Extending Time Limit Pursuant to 50 U.S.C. § 1881a(j)(2) at 1 ("May Motion"). The period for FISC review of Certification [REDACTED] was then set to expire on May 20, 2011, and the period for review of the other pending certifications and amendments was set to expire on May 22, 2011. Id. at 6.<sup>5</sup>

The government noted in the May Motion that its efforts to address the issues raised in the May 2 Letter were still ongoing and that it intended to "supplement the record . . . in a manner that will aid the Court in its review" of the certifications and amendments and in making the determinations required under Section 702. Id. at 7. According to the May Motion, however, the government would "not be in a position to supplement the record until after the statutory time limits for such review have expired." Id. The government further asserted that granting the requested extension of time would be consistent with national security, because, by operation of

---

<sup>5</sup> 50 U.S.C. § 1881a(i)(1)(B) requires the Court to complete its review of the certification and accompanying targeting and minimization procedures and issue an order under subsection 1881a(i)(3) not later than 30 days after the date on which the certification and procedures are submitted. Pursuant to subsection 1881a(i)(1)(C), the same time limit applies to review of an amended certification or amended procedures. However, 50 U.S.C. § 1881a(j)(2) permits the Court, by order for reasons stated, to extend "as necessary for good cause in a manner consistent with national security," the time limit for the Court to complete its review and issue an order under Section 1881a(i)(3).

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

statute, the government's acquisition of foreign intelligence information under Certifications [REDACTED] could continue pending completion of the Court's review. See id. at 9-10.

On May 9, 2011, the Court entered orders granting the government's May Motion. Based upon the representations in the motion, the Court found that there was good cause to extend the time limit for its review of the certifications to July 22, 2011, and that the extensions were consistent with national security. May 9, 2011 Orders at 4.

D. The May 9 Briefing Order

Because it appeared to the Court that the acquisitions described in the May 2 Letter exceeded the scope of collection previously disclosed by the government and approved by the Court, and might, in part, fall outside the scope of Section 702, the Court issued a Briefing Order on May 9, 2011 ("Briefing Order"), in which it directed the government to answer a number of questions in writing. Briefing Order at 3-5. On June 1, 2011, the United States filed the "Government's Response to the Court's Briefing Order of May 9, 2011" ("June 1 Submission"). After reviewing the June 1 Submission, the Court, through its staff, directed the government to answer a number of follow-up questions. On June 28, 2011, the government submitted its written responses to the Court's follow-up questions in the "Government's Response to the Court's Follow-Up Questions of June 17, 2011" ("June 28 Submission").

E. The Government's Second Motion for Extensions of Time

The Court met with senior officials of the Department of Justice on July 8, 2011, to

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

discuss the information provided by the government in the June 1 and June 28 Submissions. During the meeting, the Court informed the government that it still had serious concerns regarding NSA's acquisition of Internet transactions and, in particular, whether the Court could make the findings necessary to approve the acquisition of such transactions pursuant to Section 702. The Court also noted its willingness to entertain any additional filings that the government might choose to make in an effort to address those concerns.

On July 14, 2011, the government filed a motion seeking additional sixty-day extensions of the periods in which the Court must complete its review of DNI/AG 702(g) Certifications [REDACTED], and the amendments to the certifications in the Prior 702 Dockets. Motion for Orders Extending Time Limits Pursuant to 50 U.S.C. § 1881a(j)(2) ("July Motion").<sup>6</sup>

In its July Motion, the government indicated that it was in the process of compiling additional information regarding the nature and scope of NSA's upstream collection, and that it was "examining whether enhancements to NSA's systems or processes could be made to further ensure that information acquired through NSA's upstream collection is handled in accordance with the requirements of the Act." *Id.* at 8. Because additional time would be needed to supplement the record, however, the government represented that a 60-day extension would be necessary. *Id.* at 8, 11. The government argued that granting the request for an additional extension of time would be consistent with national security, because, by operation of statute, the

---

<sup>6</sup> As discussed above, by operation of the Court's order of May 9, 2011, pursuant to 50 U.S.C. § 1881a(j)(2), the Court was required to complete its review of, and issue orders under 50 U.S.C. § 1881a(i)(3) concerning, DNI/AG 702(g) Certifications [REDACTED] and the amendments to the certifications in the Prior 702 Dockets, by July 22, 2011. *Id.* at 6.

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

government's acquisition of foreign intelligence information under Certifications [REDACTED]

[REDACTED] could continue pending completion of the Court's review. *Id.* at 9-10.

On July 14, 2011, the Court entered orders granting the government's motion. Based upon the representations in the motion, the Court found that there was good cause to extend the time limit for its review of the certifications to September 20, 2011, and that the extensions were consistent with national security. July 14, 2011 Orders at 4.

F. The August 16 and August 30 Submissions

On August 16, 2011, the government filed a supplement to the June 1 and June 28 Submissions ("August 16 Submission"). In the August 16 Submission, the government described the results of "a manual review by [NSA] of a statistically representative sample of the nature and scope of the Internet communications acquired through NSA's . . . Section 702 upstream collection during a six-month period." Notice of Filing of Aug. 16 Submission at 2. Following a meeting between the Court staff and representatives of the Department of Justice on August 22, 2011, the government submitted a further filing on August 30, 2011 ("August 30 Submission").

G. The Hearing and the Government's Final Written Submission

Following review of the August 30 Submission, the Court held a hearing on September 7, 2011, to ask additional questions of NSA and the Department of Justice regarding the government's statistical analysis and the implications of that analysis. The government made its

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

final written submissions on September 9, 2011, and September 13, 2011 (“September 9 Submission” and “September 13 Submission,” respectively).

H. The Final Extension of Time

On September 14, 2011, the Court entered orders further extending the deadline for its completion of the review of the certifications and amendments filed as part of the April Submissions. The Court explained that “[g]iven the complexity of the issues presented in these matters coupled with the Court’s need to fully analyze the supplemental information provided by the government in recent filings, the last of which was submitted to the Court on September 13, 2011, the Court will not be able to complete its review of, and issue orders . . . concerning [the certifications and amendments] by September 20, 2011.” [REDACTED]

[REDACTED] The Court further explained that although it had originally intended to extend the deadline by only one week, the government had advised the Court that “for technical reasons, such a brief extension would compromise the government’s ability to ensure a seamless transition from one Certification to the next.” [REDACTED]

[REDACTED] Accordingly, the Court extended the deadline to October 10, 2011. [REDACTED]

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

II. REVIEW OF CERTIFICATIONS [REDACTED]

The Court must review a certification submitted pursuant to Section 702 of FISA “to determine whether [it] contains all the required elements.” 50 U.S.C. § 1881a(i)(2)(A). The Court’s examination of Certifications [REDACTED] confirms that:

- (1) the certifications have been made under oath by the Attorney General and the DNI, as required by 50 U.S.C. § 1881a(g)(1)(A), see Certification [REDACTED];
- (2) the certifications contain each of the attestations required by 50 U.S.C. § 1881a(g)(2)(A), see Certification [REDACTED];
- (3) as required by 50 U.S.C. § 1881a(g)(2)(B), each of the certifications is accompanied by the applicable targeting procedures<sup>7</sup> and minimization procedures;<sup>8</sup>
- (4) each of the certifications is supported by the affidavits of appropriate national security officials, as described in 50 U.S.C. § 1881a(g)(2)(C);<sup>9</sup> and
- (5) each of the certifications includes an effective date for the authorization in compliance

---

<sup>7</sup> See April 2011 Submissions, NSA Targeting Procedures and FBI Targeting Procedures (attached to Certifications [REDACTED]).

<sup>8</sup> See April 2011 Submissions, NSA Minimization Procedures, FBI Minimization Procedures, and CIA Minimization Procedures (attached to Certifications [REDACTED]).

<sup>9</sup> See April 2011 Submissions, Affidavits of John C. Inglis, Acting Director, NSA (attached to Certifications [REDACTED]); Affidavit of Gen. Keith B. Alexander, U.S. Army, Director, NSA (attached to Certification [REDACTED]); Affidavits of Robert S. Mueller, III, Director, FBI (attached to Certifications [REDACTED]); [REDACTED]

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

with 50 U.S.C. § 1881a(g)(2)(D), see Certification [REDACTED]

<sup>10</sup>

The Court therefore finds that Certification [REDACTED]

[REDACTED] contain all the required elements. 50 U.S.C. § 1881a(i)(2)(A).

III. REVIEW OF THE AMENDMENTS TO THE CERTIFICATIONS IN THE PRIOR DOCKETS.

Under the judicial review procedures that apply to amendments by virtue of Section 1881a(i)(1)(C), the Court must review each of the amended certifications "to determine whether the certification contains all the required elements." 50 U.S.C. § 1881a(i)(2)(A). The Court has previously determined that the certifications in each of the Prior 702 Dockets, as originally submitted to the Court and previously amended, contained all the required elements.<sup>11</sup> Like the prior certifications and amendments, the amendments now before the Court were executed under oath by the Attorney General and the DNI, as required by 50 U.S.C. § 1881a(g)(1)(A), and submitted to the Court within the time allowed under 50 U.S.C. § 1881a(i)(1)(C). See

---

<sup>10</sup> The statement described in 50 U.S.C. § 1881a(g)(2)(E) is not required in this case because there has been no "exigent circumstances" determination under Section 1881a(c)(2).

<sup>11</sup> [REDACTED]

~~TOP SECRET//COMINT//ORCON,NOFORN~~



~~TOP SECRET//COMINT//ORCON,NOFORN~~

Certification [REDACTED]<sup>12</sup> Pursuant to Section 1881a(g)(2)(A)(ii), the latest amendments include the attestations of the Attorney General and the DNI that the accompanying NSA and CIA minimization procedures meet the statutory definition of minimization procedures, are consistent with the requirements of the Fourth Amendment, and will be submitted to the Court for approval. Certification [REDACTED]  
[REDACTED]. The latest amendments also include effective dates that comply with 50 U.S.C. § 1881a(g)(2)(D) and § 1881a(i)(1).

Certification [REDACTED] All other aspects of the certifications in the Prior 702 Dockets – including the further attestations made therein in accordance with § 1881a(g)(2)(A), the NSA targeting procedures and FBI minimization procedures submitted therewith in accordance with § 1881a(g)(2)(B),<sup>13</sup> and the affidavits executed in support thereof in accordance with § 1881a(g)(2)(C) – are unaltered by the latest amendments.

In light of the foregoing, the Court finds that the certifications in the Prior 702 Dockets, as amended, each contain all the required elements, 50 U.S.C. § 1881a(i)(2)(A).

---

<sup>12</sup> The amendments to the certifications in the Prior 702 Dockets were approved by the Attorney General on April 11, 2011, and by the DNI on April 13, 2011. See Certification [REDACTED]  
[REDACTED]

<sup>13</sup> Of course, targeting under the certifications filed in the Prior 702 Dockets will no longer be permitted following the Court's issuance of an order on Certifications [REDACTED]  
[REDACTED]

~~TOP SECRET//COMINT//ORCON,NOFORN~~

IV. REVIEW OF THE TARGETING AND MINIMIZATION PROCEDURES

The Court is required to review the targeting and minimization procedures to determine whether they are consistent with the requirements of 50 U.S.C. § 1881a(d)(1) and (e)(1). See 50 U.S.C. § 1881a(i)(2)(B) and (C); see also 50 U.S.C. § 1881a(i)(1)(C) (providing that amended procedures must be reviewed under the same standard). Section 1881a(d)(1) provides that the targeting procedures must be “reasonably designed” to “ensure that any acquisition authorized under [the certification] is limited to targeting persons reasonably believed to be located outside the United States” and to “prevent the intentional acquisition of any communication as to which the sender and all intended recipients are known at the time of the acquisition to be located in the United States.” Section 1881a(e)(1) requires that the minimization procedures “meet the definition of minimization procedures under [50 U.S.C. §§] 1801(h) or 1821(4) . . . .” Most notably, that definition requires “specific procedures, which shall be adopted by the Attorney General, that are reasonably designed in light of the purpose and technique of the particular [surveillance or physical search], to minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information.” 50 U.S.C. §§ 1801(h) & 1821(4). Finally, the Court must determine whether the targeting and minimization procedures are consistent with the requirements of the Fourth Amendment. 50 U.S.C. § 1881a(i)(3)(A).

~~TOP SECRET//COMINT//ORCON,NOFORN~~

A. The Effect of the Government's Disclosures Regarding NSA's Acquisition of Internet Transactions on the Court's Review of the Targeting and Minimization Procedures

The Court's review of the targeting and minimization procedures submitted with the April 2011 Submissions is complicated by the government's recent revelation that NSA's acquisition of Internet communications through its upstream collection under Section 702 is accomplished by acquiring Internet "transactions," which may contain a single, discrete communication, or multiple discrete communications, including communications that are neither to, from, nor about targeted facilities. June 1 Submission at 1-2. That revelation fundamentally alters the Court's understanding of the scope of the collection conducted pursuant to Section 702 and requires careful reexamination of many of the assessments and presumptions underlying its prior approvals.

In the first Section 702 docket, [REDACTED], the government disclosed that its Section 702 collection would include both telephone and Internet communications. According to the government, the acquisition of telephonic communications would be limited to "to/from" communications -- i.e., communications to or from a tasked facility. The government explained, however, that the Internet communications acquired would include both to/from communications and "about" communications -- i.e., communications containing a reference to the name of the tasked account. See [REDACTED]. Based upon the government's descriptions of the proposed collection, the Court understood that the acquisition of Internet communications under Section 702 would be limited to discrete "to/from" communications between or among individual account users and to "about"

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

communications falling within [REDACTED] specific categories that had been first described to the Court in prior proceedings. [REDACTED]

[REDACTED] The Court's analysis and ultimate approval of the targeting and minimization procedures in Docket No. [REDACTED], and in the other [REDACTED] Prior 702 Dockets, depended upon the government's representations regarding the scope of the collection. In conducting its review and granting those approvals, the Court did not take into account NSA's acquisition of Internet transactions, which now materially and fundamentally alters the statutory and constitutional analysis.<sup>14</sup>

---

<sup>14</sup> The Court is troubled that the government's revelations regarding NSA's acquisition of Internet transactions mark the third instance in less than three years in which the government has disclosed a substantial misrepresentation regarding the scope of a major collection program.

In March, 2009, the Court concluded that its authorization of NSA's bulk acquisition of telephone call detail records from [REDACTED] in the so-called "big business records" matter "ha[d] been premised on a flawed depiction of how the NSA uses [the acquired] metadata," and that "[t]his misperception by the FISC existed from the inception of its authorized collection in May 2006, buttressed by repeated inaccurate statements made in the government's submissions, and despite a government-devised and Court-mandated oversight regime." Docket [REDACTED] Contrary to the government's repeated assurances, NSA had been routinely running queries of the metadata using querying terms that did not meet the required standard for querying. The Court concluded that this requirement had been "so frequently and systemically violated that it can fairly be said that this critical element of the overall . . . regime has never functioned effectively." *Id.*

[REDACTED]

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

The government's submissions make clear not only that NSA has been acquiring Internet transactions since before the Court's approval of the first Section 702 certification in 2008,<sup>15</sup> but also that NSA seeks to continue the collection of Internet transactions. Because NSA's acquisition of Internet transactions presents difficult questions, the Court will conduct its review in two stages. Consistent with the approach it has followed in past reviews of Section 702 certifications and amendments, the Court will first consider the targeting and minimization procedures as applied to the acquisition of communications other than Internet transactions – i.e., to the discrete communications between or among the users of telephone and Internet communications facilities that are to or from a facility tasked for collection.<sup>16</sup> The Court will

<sup>14</sup> [REDACTED]

<sup>15</sup> The government's revelations regarding the scope of NSA's upstream collection implicate 50 U.S.C. § 1809(a), which makes it a crime (1) to "engage[] in electronic surveillance under color of law except as authorized" by statute or (2) to "disclose[] or use[] information obtained under color of law by electronic surveillance, knowing or having reason to know that the information was obtained through electronic surveillance not authorized" by statute. See [REDACTED] (concluding that Section 1809(a)(2) precluded the Court from approving the government's proposed use of, among other things, certain data acquired by NSA without statutory authority through its "upstream collection"). The Court will address Section 1809(a) and related issues in a separate order.

<sup>16</sup> As noted, the Court previously authorized the acquisition of [REDACTED] categories of "about" communications. The Court now understands that all "about" communications are acquired by means of NSA's acquisition of Internet transactions through its upstream collection. See June 1 Submission at 1-2, see also Sept. 7, 2011 Hearing Tr. at 76. Accordingly, the Court considers the  
(continued...)

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

then assess the effect of the recent disclosures regarding NSA's collection of Internet transactions on its ability to make the findings necessary to approve the certifications and the NSA targeting and minimization procedures.<sup>17</sup>

**B. The Unmodified Procedures**

The government represents that the NSA targeting procedures and the FBI minimization procedures filed with the April 2011 Submissions are identical to the corresponding procedures that were submitted to the Court in Docket Nos. [REDACTED].<sup>18</sup>

The Court has reviewed each of these sets of procedures and confirmed that is the case. In fact, the NSA targeting procedures and FBI minimization procedures now before the Court are copies

---

<sup>16</sup>(...continued)

[REDACTED] categories of "about" communications to be a subset of the Internet transactions that NSA acquires. The Court's discussion of the manner in which the government proposes to apply its targeting and minimization procedures to Internet transactions generally also applies to the [REDACTED] categories of "about" communications. See *infra*, pages 41-79.

<sup>17</sup> The FBI and the CIA do not receive unminimized communications that have been acquired through NSA's upstream collection of Internet communications. Sept. 7, 2011 Hearing Tr. at 61-62. Accordingly, the discussion of Internet transactions that appears below does not affect the Court's conclusions that the FBI targeting procedures, the CIA minimization procedures, and the FBI minimization procedures meet the statutory and constitutional requirements.

<sup>18</sup> See Government's Ex Parte Submission of Reauthorization Certification and Related Procedures, Ex Parte Submission of Amended Certifications, and Request for an Order Approving Such Certification and Amended Certifications for DNI/AG 702(g) Certifications [REDACTED]; Government's Ex Parte Submission of Reauthorization Certification and Related Procedures, Ex Parte Submission of Amended Certifications, and Request for an Order Approving Such Certification and Amended Certifications for DNI/AG 702(g) Certifications [REDACTED]; Government's Ex Parte Submission of Reauthorization Certification and Related Procedures, Ex Parte Submission of Amended Certifications, and Request for an Order Approving Such Certification and Amended Certifications for DNI/AG 702(g) Certifications [REDACTED].

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

of the procedures that were initially filed on July 29, 2009, in Docket No. [REDACTED]<sup>19</sup> The Court found in those prior dockets that the targeting and minimization procedures were consistent with the requirements of 50 U.S.C. § 1881a(d)-(e) and with the Fourth Amendment. See Docket No. [REDACTED]

[REDACTED] The Court is prepared to renew its past findings that the NSA targeting procedures (as applied to forms of to/from communications that have previously been described to the Court) and the FBI minimization procedures are consistent with the requirements of 50 U.S.C. § 1881a(d)-(e) and with the Fourth Amendment.<sup>20</sup>

C. The Amended Procedures

As noted above, the FBI targeting procedures and the NSA and CIA minimization procedures submitted with the April 2011 Submissions differ in a number of respects from the corresponding procedures that were submitted by the government and approved by the Court in connection with Certifications [REDACTED]. For the reasons that follow, the Court finds that, as applied to the previously authorized collection of discrete communications to or from a tasked facility, the amended FBI targeting procedures and the amended NSA and CIA

---

<sup>19</sup> Copies of those same procedures were also submitted in Docket Nos. [REDACTED]

<sup>20</sup> The Court notes that the FBI minimization procedures are not "set forth in a clear and self-contained manner, without resort to cross-referencing," as required by FISC Rule 12, which became effective on November 1, 2010. The Court expects that future submissions by the government will comport with this requirement.

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

minimization procedures are consistent with the requirements of 50 U.S.C. § 1881a(d)-(e) and with the Fourth Amendment.

1. The Amended FBI Targeting Procedures

The government has made three changes to the FBI targeting procedures, all of which involve Section I.4. That provision requires the FBI, [REDACTED]

[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]

The new language proposed by the government would allow the FBI to [REDACTED]

[REDACTED]

[REDACTED] The government has advised the Court that this change was prompted by the fact that [REDACTED]

[REDACTED] Nevertheless, the current procedures require the FBI to [REDACTED]. The change is intended to eliminate the requirement of [REDACTED].

The second change, reflected in subparagraph (a) of Section I.4, would allow the FBI, under certain circumstances, to [REDACTED]

[REDACTED]

~~TOP SECRET//COMINT//ORCON,NOFORN~~



~~TOP SECRET//COMINT//ORCON,NOFORN~~

[REDACTED]

The above-described changes to the FBI targeting procedures pose no obstacle to a finding by the Court that the FBI targeting procedures are “reasonably designed” to “ensure that any acquisition authorized . . . is limited to targeting persons reasonably believed to be located outside the United States” and to “prevent the intentional acquisition of any communication as to which the sender and all intended recipients are known at the time of the acquisition to be located in the United States.” 50 U.S.C. § 1881a(d)(1). [REDACTED]

[REDACTED]

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

[REDACTED]

[REDACTED]

Furthermore, as the Court has previously noted, before the FBI targeting procedures are applied, NSA will have followed its own targeting procedures in determining that the user of the facility to be tasked for collection is a non-United States person reasonably believed to be located outside the United States. See Docket No. [REDACTED]. The

[REDACTED]

[REDACTED] Id. The Court has previously found that [REDACTED] [REDACTED] proposed for use in connection with Certifications [REDACTED] are reasonably designed to ensure that the users of tasked selectors are non-United States persons reasonably believed to be located outside the United States and also consistent with the Fourth Amendment. See Docket No. [REDACTED]. It therefore follows that the amended FBI targeting procedures, which provide additional assurance that the users of tasked accounts are non-United States persons located outside the United States, also pass muster.

2. The Amended NSA Minimization Procedures

The most significant change to the NSA minimization procedures regards the rules for querying the data that NSA acquires pursuant to Section 702. The procedures previously approved by the Court effectively impose a wholesale bar on queries using United States-Person identifiers. The government has broadened Section 3(b)(5) to allow NSA to query the vast majority of its Section 702 collection using United States-Person identifiers, subject to approval

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

pursuant to internal NSA procedures and oversight by the Department of Justice.<sup>21</sup> Like all other NSA queries of the Section 702 collection, queries using United States-person identifiers would be limited to those reasonably likely to yield foreign intelligence information. NSA Minimization Procedures § 3(b)(5). The Department of Justice and the Office of the DNI would be required to conduct oversight regarding NSA's use of United States-person identifiers in such queries. See id.

This relaxation of the querying rules does not alter the Court's prior conclusion that NSA minimization procedures meet the statutory definition of minimization procedures. [REDACTED]

[REDACTED]

[REDACTED] contain an analogous provision allowing queries of unminimized FISA-acquired information using identifiers – including United States-person identifiers – when such queries are designed to yield foreign intelligence information.

See [REDACTED] In granting [REDACTED] applications for electronic surveillance or physical search since 2008, including applications targeting United States persons and persons in the United States, the Court has found that the [REDACTED] meet the definitions of minimization procedures at 50 U.S.C. §§ 1801(h) and 1821(4). It follows that the substantially-similar

---

<sup>21</sup> The government is still in the process of developing its internal procedures and will not permit NSA analysts to begin using United States-person identifiers as selection terms until those procedures are completed. June 28 Submission at 4 n.3. In addition, the government has clarified that United States-person identifiers will not be used to query the fruits of NSA's upstream collection. Aug. 30 Submission at 11. NSA's upstream collection acquires approximately 9% of the total Internet communications acquired by NSA under Section 702. Aug. 16 Submission at 2.

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

querying provision found at Section 3(b)(5) of the amended NSA minimization procedures should not be problematic in a collection that is focused on non-United States persons located outside the United States and that, in the aggregate, is less likely to result in the acquisition of nonpublic information regarding non-consenting United States persons.

A second change to the NSA minimization procedures is the addition of language specifying that the five-year retention period for communications that are not subject to earlier destruction runs from the expiration date of the certification authorizing the collection. See NSA Minimization Procedures, §§ 3(b)(1), 3(c), 5(3)(b), and 6(a)(1)(b). The NSA minimization procedures that were previously approved by the Court included a retention period of five years, but those procedures do not specify when the five-year period begins to run. The change proposed here harmonizes the procedures with the corresponding provision of the [REDACTED] minimization procedures for Section 702 that has already been approved by the Court. See [REDACTED] Minimization Procedures at 3 (¶j).

The two remaining changes to the NSA minimization procedures are intended to clarify the scope of the existing procedures. The government has added language to Section 1 to make explicit that the procedures apply not only to NSA employees, but also to any other persons engaged in Section 702-related activities that are conducted under the direction, authority or control of the Director of NSA. NSA Minimization Procedures at 1. According to the government, this new language is intended to clarify that Central Security Service personnel conducting signals intelligence operations authorized by Section 702 are bound by the procedures, even when they are deployed with a military unit and subject to the military chain of

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

command. The second clarifying amendment is a change to the definition of "identification of a United States person" in Section 2. The new language eliminates a potential ambiguity that might have resulted in the inappropriate treatment of the name, unique title, or address of a United States person as non-identifying information in certain circumstances. *Id.* at 2. These amendments, which resolve any arguable ambiguity in favor of broader application of the protections found in the procedures, raise no concerns.

3. The Amended CIA Minimization Procedures

The CIA minimization procedures include a new querying provision [REDACTED]

[REDACTED] The new language would allow the CIA to conduct queries of Section 702-acquired information using United States-person identifiers. All CIA queries of the Section 702 collection would be subject to review by the Department of Justice and the Office of the DNI. [REDACTED]

[REDACTED], the addition of the new CIA querying provision does not preclude the Court from concluding that the amended CIA minimization procedures satisfy the statutory definition of minimization procedures and comply with the Fourth Amendment.<sup>22</sup>

The amended CIA minimization procedures include [REDACTED]

---

<sup>22</sup> The Court understands that NSA does not share its upstream collection in unminimized form with the CIA. [REDACTED]

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

[REDACTED]

[REDACTED] raises no concerns in the context of the CIA minimization procedures.

[REDACTED]

The government also has added [REDACTED]

[REDACTED]

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

[REDACTED] It likewise raises no Fourth Amendment problem. [REDACTED]  
[REDACTED]  
[REDACTED]

Finally, a new provision [REDACTED]

[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]

[REDACTED] [REDACTED] The Court likewise sees no problem with the addition  
[REDACTED] to the CIA minimization procedures.

D. The Effect of the Government's Disclosures Regarding NSA's Acquisition of Internet Transactions

Based on the government's prior representations, the Court has previously analyzed NSA's targeting and minimization procedures only in the context of NSA acquiring discrete communications. Now, however, in light of the government's revelations as to the manner in which NSA acquires Internet communications, it is clear that NSA acquires "Internet

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

transactions,<sup>23</sup> including transactions that contain a single discrete communication ("Single Communication Transactions" or "SCTs"), and transactions that contain multiple discrete communications ("Multi-[C]ommunication Transactions" or "MCTs"), see Aug. 16 Submission at 1.

The Court has repeatedly noted that the government's targeting and minimization procedures must be considered in light of the communications actually acquired. See Docket No. [REDACTED] ("Substantial implementation problems can, notwithstanding the government's intent, speak to whether the applicable targeting procedures are 'reasonably designed' to acquire only the communications of non-U.S. persons outside the United States."), see also Docket No. [REDACTED]. Until now, the Court had a singular understanding of the nature of NSA's acquisitions under Section 702. Accordingly, analysis of the implementation of the procedures focused on whether NSA's procedures were applied effectively in that context and whether the procedures adequately addressed over-collections that occurred. But, for the first time, the government has now advised the Court that the volume and nature of the information it has been collecting is fundamentally different from what the Court had been led to believe. Therefore, the Court must, as a matter of first impression, consider whether, in view of NSA's acquisition of Internet transactions, the targeting and minimization procedures satisfy the statutory standards and comport with the

---

<sup>23</sup> The government describes an Internet "transaction" as "a complement of 'packets' traversing the Internet that together may be understood by a device on the Internet and, where applicable, rendered in an intelligible form to the user of that device." June 1 Submission at 1.

~~TOP SECRET//COMINT//ORCON,NOFORN~~



~~TOP SECRET//COMINT//ORCON,NOFORN~~

Fourth Amendment.

For the reasons set forth below, the Court finds that NSA's targeting procedures, as the government proposes to implement them in connection with MCTs, are consistent with the requirements of 50 U.S.C. §1881a(d)(1). However, the Court is unable to find that NSA's minimization procedures, as the government proposes to apply them in connection with MCTs, are "reasonably designed in light of the purpose and technique of the particular [surveillance or physical search], to minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information." 50 U.S.C. §§ 1801(h)(1) & 1821(4)(A). The Court is also unable to find that NSA's targeting and minimization procedures, as the government proposes to implement them in connection with MCTs, are consistent with the Fourth Amendment.

1. The Scope of NSA's Upstream Collection

NSA acquires more than two hundred fifty million Internet communications each year pursuant to Section 702, but the vast majority of these communications are obtained from Internet service providers and are not at issue here.<sup>24</sup> Sept. 9 Submission at 1; Aug. 16 Submission at Appendix A. Indeed, NSA's upstream collection constitutes only approximately

---

<sup>24</sup> In addition to its upstream collection, NSA acquires discrete Internet communications from Internet service providers such as [REDACTED] [REDACTED] Aug. 16 Submission at 2; Aug. 30 Submission at 11; see also Sept. 7, 2011 Hearing Tr. at 75-77. NSA refers to this non-upstream collection as its "PRISM collection." Aug. 30 Submission at 11. The Court understands that NSA does not acquire "Internet transactions" through its PRISM collection. See Aug. 16 Submission at 1.

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

9% of the total Internet communications being acquired by NSA under Section 702. Sept. 9 Submission at 1; Aug. 16 Submission at 2.

Although small in relative terms, NSA's upstream collection is significant for three reasons. First, NSA's upstream collection is "uniquely capable of acquiring certain types of targeted communications containing valuable foreign intelligence information."<sup>25</sup> Docket No. [REDACTED]

Second, the Court now understands that, in order to collect those targeted Internet communications, NSA's upstream collection devices acquire Internet transactions, and NSA acquires millions of such transactions each year.<sup>26</sup> Third, the government has acknowledged that, due to the technological challenges associated with acquiring Internet transactions, NSA is unable to exclude certain Internet transactions from its upstream collection. See June 1 Submission at 3-12.

In its June 1 Submission, the government explained that NSA's upstream collection devices have technological limitations that significantly affect the scope of collection. [REDACTED]

[REDACTED]

<sup>25</sup> [REDACTED]

<sup>26</sup> NSA acquired more than 13.25 million Internet transactions through its upstream collection between January 1, 2011, and June 30, 2011. See Aug. 16 Submission at 2; see also Sept. 9 Submission at 1-2.

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

[REDACTED]. See id. at 7. Moreover, at the time of acquisition, NSA's upstream Internet collection devices are generally incapable of distinguishing between transactions containing only a single discrete communication to, from, or about a tasked selector and transactions containing multiple discrete communications, not all of which may be to, from, or about a tasked selector.<sup>27</sup> Id. at 2.

As a practical matter, this means that NSA's upstream collection devices acquire any Internet transaction transiting the device if the transaction contains a targeted selector anywhere within it, and:

[REDACTED]

See id. at 6.

The practical implications of NSA's acquisition of Internet transactions through its upstream collection for the Court's statutory and Fourth Amendment analyses are difficult to assess. The sheer volume of transactions acquired by NSA through its upstream collection is such that any meaningful review of the entire body of the transactions is not feasible. As a result, the Court cannot know for certain the exact number of wholly domestic communications acquired through this collection, nor can it know the number of non-target communications

[REDACTED]

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

acquired or the extent to which those communications are to or from United States persons or persons in the United States. Instead, NSA and the Court can only look at samples of the data and then draw whatever reasonable conclusions they can from those samples. Even if the Court accepts the validity of conclusions derived from statistical analyses, there are significant hurdles in assessing NSA's upstream collection. Internet service providers are constantly changing their protocols and the services they provide, and often give users the ability to customize how they use a particular service.<sup>28</sup> *Id.* at 24-25. As a result, it is impossible to define with any specificity the universe of transactions that will be acquired by NSA's upstream collection at any point in the future.

Recognizing that further revelations concerning what NSA has actually acquired through its 702 collection, together with the constant evolution of the Internet, may alter the Court's analysis at some point in the future, the Court must, nevertheless, consider whether NSA's targeting and minimization procedures are consistent with FISA and the Fourth Amendment based on the record now before it. In view of the revelations about how NSA is actually conducting its upstream collection, two fundamental underpinnings of the Court's prior assessments no longer hold true.

---

28 [REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

First, the Court previously understood that NSA's technical measures<sup>29</sup> would prevent the acquisition of any communication as to which the sender and all intended recipients were located in the United States ("wholly domestic communication") except for "theoretically possible" cases

[REDACTED]

[REDACTED]

[REDACTED] The Court now understands, however, that NSA has acquired, is acquiring, and, if the certifications and procedures now before the Court are approved, will continue to acquire, tens of thousands of wholly domestic communications. NSA's manual review of a statistically representative sample drawn from its upstream collection<sup>30</sup> reveals that NSA acquires approximately 2,000-10,000 MCTs each year that contain at least one wholly domestic communication.<sup>31</sup> See Aug. 16 Submission at 9. In addition to these MCTs, NSA

---

<sup>29</sup> [REDACTED]

<sup>30</sup> In an effort to address the Court's concerns, NSA conducted a manual review of a random sample consisting of 50,440 Internet transactions taken from the more than 13.25 million Internet transactions acquired through NSA's upstream collection during a six month period. See generally Aug. 16 Submission (describing NSA's manual review and the conclusions NSA drew therefrom). The statistical conclusions reflected in this Memorandum Opinion are drawn from NSA's analysis of that random sample.

<sup>31</sup> Of the approximately 13.25 million Internet transactions acquired by NSA through its upstream collection during the six-month period, between 996 and 4,965 are MCTs that contain a wholly domestic communication not to, from, or about a tasked selector. Aug. 16 Submission at 9.

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

likely acquires tens of thousands more wholly domestic communications every year,<sup>32</sup> given that NSA's upstream collection devices will acquire a wholly domestic "about" SCT if it is routed internationally.<sup>33</sup> Moreover, the actual number of wholly domestic communications acquired

---

<sup>32</sup> NSA's manual review focused on examining the MCTs acquired through NSA's upstream collection in order to assess whether any contained wholly domestic communications. Sept. 7, 2011 Hearing Tr. at 13-14. As a result, once NSA determined that a transaction contained a single, discrete communication, no further analysis of that transaction was done. See Aug. 16 Submission at 3. After the Court expressed concern that this category of transactions might also contain wholly domestic communications, NSA conducted a further review. See Sept. 9 Submission at 4. NSA ultimately did not provide the Court with an estimate of the number of wholly domestic "about" SCTs that may be acquired through its upstream collection. Instead, NSA has concluded that "the probability of encountering wholly domestic communications in transactions that feature only a single, discrete communication should be smaller -- and certainly no greater -- than potentially encountering wholly domestic communications within MCTs." Sept. 13 Submission at 2.

The Court understands this to mean that the percentage of wholly domestic communications within the universe of SCTs acquired through NSA's upstream collection should not exceed the percentage of MCTs containing a wholly domestic communication that NSA found when it examined all of the MCTs within its statistical sample. Since NSA found 10 MCTs with wholly domestic communications within the 5,081 MCTs reviewed, the relevant percentage is .197% (10/5,081), Aug. 16 Submission at 5.

NSA's manual review found that approximately 90% of the 50,440 transactions in the sample were SCTs. Id. at 3. Ninety percent of the approximately 13.25 million total Internet transactions acquired by NSA through its upstream collection during the six-month period, works out to be approximately 11,925,000 transactions. Those 11,925,000 transactions would constitute the universe of SCTs acquired during the six-month period, and .197% of that universe would be approximately 23,000 wholly domestic SCTs. Thus, NSA may be acquiring as many as 46,000 wholly domestic "about" SCTs each year, in addition to the 2,000-10,000 MCTs referenced above.

<sup>33</sup> Internet communications are "nearly always transmitted from a sender to a recipient through multiple legs before reaching their final destination." June 1 Submission at 6. For example, an e-mail message sent from the user of [REDACTED] to the user of [REDACTED] will at the very least travel from the [REDACTED] user's own computer, to [REDACTED], to [REDACTED], and then to the computer of the [REDACTED] user. Id. Because the communication's route is made up of multiple legs, the transaction used to transmit the communication across any particular leg of the route need only identify the IP

(continued...)

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

may be still higher in view of NSA's inability conclusively to determine whether a significant portion of the MCTs within its sample contained wholly domestic communications.<sup>34</sup>

Second, the Court previously understood that NSA's upstream collection would only acquire the communication of a United States person or a person in the United States if: 1) that

---

<sup>33</sup>(...continued)

addresses at either end of that leg in order to properly route the communication, *Id.* at 7. As a result, for each leg of the route, the transaction header will only contain the IP addresses at either end of that particular leg. *Id.* [REDACTED]

<sup>34</sup> During its manual review, NSA was unable to determine whether 224 of the 5,081 MCTs reviewed contained any wholly domestic communications, because the transactions lacked sufficient information for NSA to determine the location or identity of the "active user" (i.e., the individual using the electronic communications account/address/identifier to interact with his/her Internet service provider). Aug. 16 Submission at 7. NSA then conducted an intensive review of all available information for each of these MCTs, including examining the contents of each discrete communication contained within it, but was still unable to determine conclusively whether any of these MCTs contained wholly domestic communications. Sept. 9 Submission at 3. NSA asserts that "it is reasonable to presume that [the] 224 MCTs do not contain wholly domestic communications," but concedes that, due to the limitations of the technical means used to prevent the acquisition of wholly domestic communications, NSA may acquire wholly domestic communications. See Aug. 30 Submission at 7-8. The Court is prepared to accept that the number of wholly domestic communications acquired in this category of MCTs is relatively small, for the reasons stated in the government's August 30 Submission. However, when considering NSA's upstream collection as a whole, and the limitations of NSA's technical means, the Court is not prepared to presume that the number of wholly domestic communications contained within this category of communications will be zero. Accordingly, the Court concludes that this category of communications acquired through NSA's upstream collection may drive the total number of wholly domestic communications acquired slightly higher.

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

person was in direct contact with a targeted selector; 2) the communication referenced the targeted selector, and the communication fell into one of [REDACTED] specific categories of "about" communications; or 3) despite the operation of the targeting procedures, United States persons or persons inside the United States were mistakenly targeted. See Docket No. [REDACTED]. But the Court now understands that, in addition to these communications, NSA's upstream collection also acquires: a) the communications of United States persons and persons in the United States that are not to, from, or about a tasked selector and that are acquired solely because the communication is contained within an MCT that somewhere references a tasked selector [REDACTED] and b) any Internet transaction that references a targeted selector, regardless of whether the transaction falls within one of the [REDACTED] previously identified categories of "about communications," see June 1 Submission at 24-27. [REDACTED]

On the current record, it is difficult to assess how many MCTs acquired by NSA actually contain a communication of or concerning a United States person,<sup>35</sup> or a communication to or from a person in the United States. This is because NSA's manual review of its upstream collection focused primarily on wholly domestic communications – *i.e.*, if one party to the

---

<sup>35</sup> NSA's minimization procedures define "[c]ommunications of a United States person" to include "all communications to which a United States person is a party." NSA Minimization Procedures § 2(c). "Communications concerning a United States person" include "all communications in which a United States person is discussed or mentioned, except where such communications reveal only publicly-available information about the person. *Id.* § 2(b).

~~TOP SECRET//COMINT//ORCON,NOFORN~~



communication was determined to be outside the United States, the communication was not further analyzed. Aug. 16 Submission at 1-2. Nevertheless, NSA's manual review did consider the location and identity of the active user for each MCT acquired, and this information -- when considered together with certain presumptions -- shows that NSA is likely acquiring tens of thousands of discrete communications of non-target United States persons and persons in the United States, by virtue of the fact that their communications are included in MCTs selected for acquisition by NSA's upstream collection devices.<sup>36</sup>

To illustrate, based upon NSA's analysis of the location and identity of the active user for the MCTs it reviewed, MCTs can be divided into four categories:

1. MCTs as to which the active user is the user of the tasked facility (i.e., the target of the acquisition) and is reasonably believed to be located outside the United States;<sup>37</sup>
2. MCTs as to which the active user is a non-target who is believed to be located inside the United States;
3. MCTs as to which the active user is a non-target who is believed to be located outside the United States; and

---

<sup>36</sup> Although there is some overlap between this category of communications and the tens of thousands of wholly domestic communications discussed above, the overlap is limited to MCTs containing wholly domestic communications. To the extent that the wholly domestic communications acquired are SCTs, they are excluded from the MCTs referenced here. Similarly, to the extent communications of non-target United States persons and persons in the United States that are contained within the tens of thousands of MCTs referenced here are not wholly domestic, they would not be included in the wholly domestic communications referenced above.

<sup>37</sup> Although it is possible for an active user target to be located in the United States, NSA's targeting procedures require NSA to terminate collection if it determines that a target has entered the United States. NSA Targeting Procedures at 7-8. Accordingly, the Court excludes this potential category from its analysis.

4. MCTs as to which the active user's identity or location cannot be determined.

Aug. 16 Submission at 4-8.

With regard to the first category, if the target is the active user, then it is reasonable to presume that all of the discrete communications within an MCT will be to or from the target. Although United States persons and persons in the United States may be party to any of those communications, NSA's acquisition of such communications is of less concern than the communications described in the following categories because the communicants were in direct communication with a tasked facility, and the acquisition presumptively serves the foreign intelligence purpose of the collection. NSA acquires roughly 300-400 thousand such MCTs per year.<sup>38</sup>

For the second category, since the active user is a non-target who is located inside the United States, there is no reason to believe that all of the discrete communications contained within the MCTs will be to, from, or about the targeted selector (although there would need to be at least one such communication in order for NSA's upstream devices to acquire the transaction). Further, because the active user is in the United States, the Court presumes that the majority of that person's communications will be with other persons in the United States, many of whom will be United States persons. NSA acquires approximately 7,000-8,000 such MCTs per year, each of which likely contains one or more non-target discrete communications to or from other

---

<sup>38</sup> NSA acquired between 168,853 and 206,922 MCTs as to which the active user was the target over the six-month period covered by the sample. Aug. 16 Submission at 9.

persons in the United States.<sup>39</sup>

The third category is similar to the second in that the active user is a non-target. Therefore, there is no reason to believe that all of the communications within the MCTs will be to, from, or about the targeted selector (although there would need to be at least one such communication in order for NSA's upstream devices to acquire the transaction). However, because the active user is believed to be located outside the United States, the Court presumes that most of that persons's communications will be with other persons who are outside the United States, most of whom will be non-United States persons. That said, the Court notes that some of these MCTs are likely to contain non-target communications of or concerning United States persons, or that are to or from a person in the United States.<sup>40</sup> The Court has no way of knowing precisely how many such communications are acquired. Nevertheless, it appears that NSA acquires at least 1.3 million such MCTs each year,<sup>41</sup> so even if only 1% of these MCTs

---

<sup>39</sup> In its manual review, NSA identified ten MCTs as to which the active user was in the United States and that contained at least one wholly domestic communication. See Aug. 16 Submission at 5-7. NSA also identified seven additional MCTs as to which the active user was in the United States. Id. at 5. Although NSA determined that at least one party to each of the communications within the seven MCTs was reasonably believed to be located outside the United States, NSA did not indicate whether any of the communicants were United States persons or persons in the United States. Id. The Court sees no reason to treat these two categories of MCTs differently because the active users for both were in the United States. Seventeen MCTs constitutes .3% of the MCTs reviewed (5,081), and .3% of the 1.29-1.39 million MCTs NSA acquires every six months (see id. at 8) is 3,870- 4,170, or 7,740-8,340 every year.

<sup>40</sup> The government has acknowledged as much in its submissions. See June 28 Submission at 5.

<sup>41</sup> Based on its manual review, NSA assessed that 2668 of the 5,081 MCTs reviewed  
(continued...)

~~TOP SECRET//COMINT//ORCON,NOFORN~~

contain a single non-target communication of or concerning a United States person, or that is to or from a person in the United States, NSA would be acquiring in excess of 10,000 additional discrete communications each year that are of or concerning United States persons, or that are to or from a person in the United States.

The fourth category is the most problematic, because without the identity of the active user — i.e., whether the user is the target or a non-target — or the active user's location, it is difficult to determine what presumptions to make about these MCTs. NSA acquires approximately 97,000-140,000 such MCTs each year.<sup>42</sup> In the context of wholly domestic communications, the government urges the Court to apply a series of presumptions that lead to the conclusion that this category would not contain any wholly domestic communications. Aug. 30 Submission at 4-8. The Court questions the validity of those presumptions, as applied to wholly domestic communications, but certainly is not inclined to apply them to assessing the likelihood that MCTs might contain communications of or concerning United States persons, or communications to or from persons in the United States. The active users for some of these

---

<sup>41</sup>(...continued)

(approximately 52%) had a non-target active user who was reasonably believed to be located outside the United States. Aug. 16 Submission at 4-5. Fifty-two percent of the 1.29 to 1.39 million MCTs that NSA assessed were acquired through its upstream collection every six months would work out to 670,800 - 722,800 MCTs, or approximately 1.3-1.4 million MCTs per year that have a non-target active user believed to be located outside the United States.

<sup>42</sup> NSA determined that 224 MCTs of the 5,081 MCTs acquired during a six-month period [REDACTED]

[REDACTED] From this, NSA concluded that it acquired between 48,609 and 70,168 such MCTs every six months through its upstream collection (or approximately 97,000-140,000 such MCTs each year). Id. at 9 n.27.

~~TOP SECRET//COMINT//ORCON,NOFORN~~

MCTs may be located in the United States, and, even if the active user is located overseas, the MCTs may contain non-target communications of or concerning United States persons or that are to or from persons in the United States. Accordingly, this “unknown” category likely adds substantially to the number of non-target communications of or concerning United States persons or that are to or from persons in the United States being acquired by NSA each year.

In sum, then, NSA’s upstream collection is a small, but unique part of the government’s overall collection under Section 702 of the FAA. NSA acquires valuable information through its upstream collection, but not without substantial intrusions on Fourth Amendment-protected interests. Indeed, the record before this Court establishes that NSA’s acquisition of Internet transactions likely results in NSA acquiring annually tens of thousands of wholly domestic communications, and tens of thousands of non-target communications of persons who have little or no relationship to the target but who are protected under the Fourth Amendment. Both acquisitions raise questions as to whether NSA’s targeting and minimization procedures comport with FISA and the Fourth Amendment.

2. NSA’s Targeting Procedures

The Court will first consider whether NSA’s acquisition of Internet transactions through its upstream collection, as described above, means that NSA’s targeting procedures, as implemented, are not “reasonably designed” to: 1) “ensure that any acquisition authorized under [the certifications] is limited to targeting persons reasonably believed to be located outside the United States”; and 2) “prevent the intentional acquisition of any communication as to which the sender and all intended recipients are known at the time of the acquisition to be located in the

~~TOP SECRET//COMINT//ORCON,NOFORN~~

United States.” 50 U.S.C. § 1881a(d)(1); *id.* § (i)(2)(B). The Court concludes that the manner in which NSA is currently implementing the targeting procedures does not prevent the Court from making the necessary findings, and hence NSA’s targeting procedures do not offend FISA.

*a. Targeting Persons Reasonably Believed to be Located Outside the United States*

To the extent NSA is acquiring Internet transactions that contain a single discrete communication that is to, from, or about a tasked selector, the Court’s previous analysis remains valid. As explained in greater detail in the Court’s September 4, 2008 Memorandum Opinion, in this setting the person being targeted is the user of the tasked selector, and NSA’s pre-targeting and post-targeting procedures ensure that NSA will only acquire such transactions so long as there is a reasonable belief that the target is located outside the United States. Docket No. [REDACTED]

But NSA’s acquisition of MCTs complicates the Court’s analysis somewhat. With regard to “about” communications, the Court previously found that the user of the tasked facility was the “target” of the acquisition, because the government’s purpose in acquiring such communications is to obtain information about that user. *See id.* at 18. Moreover, the communication is not acquired because the government has any interest in the parties to the communication, other than their potential relationship to the user of the tasked facility, and the parties to an “about” communication do not become targets unless and until they are separately vetted under the targeting procedures. *See id.* at 18-19.

In the case of “about” MCTs – *i.e.*, MCTs that are acquired because a targeted selector is referenced somewhere in the transaction – NSA acquires not only the discrete communication

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

that references the tasked selector, but also in many cases the contents of other discrete communications that do not reference the tasked selector and to which no target is a party. See May 2 Letter at 2-3 [REDACTED] By acquiring such MCTs, NSA likely acquires tens of thousands of additional communications of non-targets each year, many of whom have no relationship whatsoever with the user of the tasked selector. While the Court has concerns about NSA's acquisition of these non-target communications, the Court accepts the government's representation that the "sole reason [a non-target's MCT] is selected for acquisition is that it contains the presence of a tasked selector used by a person who has been subjected to NSA's targeting procedures." June 1 Submission at 4. Moreover, at the time of acquisition, NSA's upstream collection devices often lack the capability to determine whether a transaction contains a single communication or multiple communications, or to identify the parties to any particular communication within a transaction. See id. Therefore, the Court has no reason to believe that NSA, by acquiring Internet transactions containing multiple communications, is targeting anyone other than the user of the tasked selector. See United States v. Chemical Found., Inc., 272 U.S. 1, 14-15 (1926) ("The presumption of regularity supports the official acts of public officers, and, in the absence of clear evidence to the contrary, courts presume that they have properly discharged their official duties.").

*b. Acquisition of Wholly Domestic Communications*

NSA's acquisition of Internet transactions complicates the analysis required by Section 1881a(d)(1)(B), since the record shows that the government knowingly acquires tens of thousands of wholly domestic communications each year. At first blush, it might seem obvious

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

that targeting procedures that permit such acquisitions could not be “reasonably designed . . . to prevent the intentional acquisition of any communication as to which the sender and all intended recipients are known at the time of the acquisition to be located in the United States.” 50 U.S.C. § 1881a(d)(1)(B). However, a closer examination of the language of the statute leads the Court to a different conclusion.

The government focuses primarily on the “intentional acquisition” language in Section 1881a(d)(1)(B). Specifically, the government argues that NSA is not “intentionally” acquiring wholly domestic communications because the government does not intend to acquire transactions containing communications that are wholly domestic and has implemented technical means to prevent the acquisition of such transactions. See June 28 Submission at 12. This argument fails for several reasons.

NSA targets a person under Section 702 certifications by acquiring communications to, from, or about a selector used by that person. Therefore, to the extent NSA’s upstream collection devices acquire an Internet transaction containing a single, discrete communication that is to, from, or about a tasked selector, it can hardly be said that NSA’s acquisition is “unintentional.” In fact, the government has argued, and the Court has accepted, that the government intentionally acquires communications to and from a target, even when NSA reasonably – albeit mistakenly – believes that the target is located outside the United States. See Docket No. [REDACTED]

With respect to MCTs, the sole reason NSA acquires such transactions is the presence of a tasked selector within the transaction. Because it is technologically infeasible for NSA’s

~~TOP SECRET//COMINT//ORCON,NOFORN~~



upstream collection devices to acquire only the discrete communication to, from, or about a tasked selector that may be contained within an MCT, however, the government argues that the only way to obtain the foreign intelligence information found within the discrete communication is to acquire the entire transaction in which it is contained. June 1 Submission at 21. As a result, the government intentionally acquires all discrete communications within an MCT, including those that are not to, from or about a tasked selector. See June 28 Submission at 12, 14; see also Sept. 7, 2011 Hearing Tr. at 33-34.

The fact that NSA's technical measures cannot prevent NSA from acquiring transactions containing wholly domestic communications under certain circumstances does not render NSA's acquisition of those transactions "unintentional." The government repeatedly characterizes such acquisitions as a "failure" of NSA's "technical means." June 28 Submission at 12; see also Sept. 7, 2011 Hearing Tr. at 35-36. However, there is nothing in the record to suggest that NSA's technical means are malfunctioning or otherwise failing to operate as designed. Indeed, the government readily concedes that NSA will acquire a wholly domestic "about" communication if the transaction containing the communication is routed through an international Internet link being monitored by NSA or is routed through a foreign server. See June 1 Submission at 29. And in the case of MCTs containing wholly domestic communications that are not to, from, or about a tasked selector, NSA has no way to determine, at the time of acquisition, that a particular communication within an MCT is wholly domestic. See id. Furthermore, now that NSA's manual review of a sample of its upstream collection has confirmed that NSA likely acquires tens of thousands of wholly domestic communications each year, there is no question that the

government is knowingly acquiring Internet transactions that contain wholly domestic communications through its upstream collection.<sup>43</sup>

The government argues that an NSA analyst's post-acquisition discovery that a particular Internet transaction contains a wholly domestic communication should retroactively render NSA's acquisition of that transaction "unintentional." June 28 Submission at 12. That argument is unavailing. NSA's collection devices are set to acquire transactions that contain a reference to the targeted selector. When the collection device acquires such a transaction, it is functioning precisely as it is intended, even when the transaction includes a wholly domestic communication. The language of the statute makes clear that it is the government's intention at the time of acquisition that matters, and the government conceded as much at the hearing in this matter. Sept. 7, 2011 Hearing Tr. at 37-38.

Accordingly, the Court finds that NSA intentionally acquires Internet transactions that reference a tasked selector through its upstream collection with the knowledge that there are tens of thousands of wholly domestic communications contained within those transactions. But this is not the end of the analysis. To return to the language of the statute, NSA's targeting procedures must be reasonably designed to prevent the intentional acquisition of "any communication as to which the sender and all intended recipients are known at the time of

---

<sup>43</sup> It is generally settled that a person intends to produce a consequence either (a) when he acts with a purpose of producing that consequence or (b) when he acts knowing that the consequence is substantially certain to occur. Restatement (Third) of Torts § 1 (2010); see also United States v. Dyer, 589 F.3d 520, 528 (1st Cir. 2009) (in criminal law, "'intent' ordinarily requires only that the defendant reasonably knew the proscribed result would occur"), cert. denied, 130 S. Ct. 2422 (2010).

~~TOP SECRET//COMINT//ORCON,NOFORN~~

acquisition to be located in the United States.” 50 U.S.C. § 1881a(d)(1)(B) (emphasis added).

The underscored language requires an acquisition-by-acquisition inquiry. Thus, the Court must consider whether, at the time NSA intentionally acquires a transaction through its upstream collection, NSA will know that the sender and all intended recipients of any particular communication within that transaction are located in the United States.

Presently, it is not technically possible for NSA to configure its upstream collection devices [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] the practical effect of this technological limitation is that NSA cannot know at the time it acquires an Internet transaction whether the sender and all intended recipients of any particular discrete communication contained within the transaction are located inside the United States.

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

---

<sup>44</sup> See *supra*, note 33.

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

[REDACTED]

Given that NSA's upstream collection devices lack the capacity to detect wholly domestic communications at the time an Internet transaction is acquired, the Court is inexorably led to the conclusion that the targeting procedures are "reasonably designed" to prevent the intentional acquisition of any communication as to which the sender and all intended recipients are known at the time of the acquisition to be located in the United States. This is true despite the fact that NSA knows with certainty that the upstream collection, viewed as a whole, results in the acquisition of wholly domestic communications.

By expanding its Section 702 acquisitions to include the acquisition of Internet transactions through its upstream collection, NSA has, as a practical matter, circumvented the spirit of Section 1881a(b)(4) and (d)(1) with regard to that collection. NSA's knowing acquisition of tens of thousands of wholly domestic communications through its upstream collection is a cause of concern for the Court. But the meaning of the relevant statutory provision is clear and application to the facts before the Court does not lead to an impossible or absurd result. The Court's review does not end with the targeting procedures, however. The Court must

~~TOP SECRET//COMINT//ORCON,NOFORN~~

also consider whether NSA's minimization procedures are consistent with §1881a(e)(1) and whether NSA's targeting and minimization procedures are consistent with the requirements of the Fourth Amendment.

3. NSA's Minimization Procedures, As Applied to MCTs in the Manner Proposed by the Government, Do Not Meet FISA's Definition of "Minimization Procedures"

The Court next considers whether NSA's minimization procedures, as the government proposes to apply them to Internet transactions, meet the statutory requirements. As noted above, 50 U.S.C. § 1881a(e)(1) requires that the minimization procedures "meet the definition of minimization procedures under [50 U.S.C. §§] 1801(h) or 1821(4) . . . ." That definition requires "specific procedures, which shall be adopted by the Attorney General, that are reasonably designed in light of the purpose and technique of the particular [surveillance or physical search], to minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information." 50 U.S.C. §§ 1801(h)(1) & 1821(4)(A). For the reasons stated below, the Court concludes that NSA's minimization procedures, as applied to MCTs in the manner proposed by the government, do not meet the statutory definition in all respects.

*a. The Minimization Framework*

NSA's minimization procedures do not expressly contemplate the acquisition of MCTs, and the language of the procedures does not lend itself to straightforward application to MCTs. Most notably, various provisions of the NSA minimization procedures employ the term

“communication” as an operative term. As explained below, for instance, the rules governing retention, handling, and dissemination vary depending whether or not a communication is deemed to constitute a “domestic communication” instead of a “foreign communication,” see NSA Minimization Procedures §§ 2(e), 5, 6, 7; a communication “of” or “concerning” a U.S. person, see id. §§ 2(b)-(c), 3(b)(1)-(2), 3(e); a “communication to, from, or about a target,” id. § 3(b)(4); or a “communication . . . reasonably believed to contain foreign intelligence information or evidence of a crime,” id. But MCTs can be fairly described as communications that contain several smaller communications. Applying the terms of the NSA minimization procedures to MCTs rather than discrete communications can produce very different results.

In a recent submission, the government explained how NSA proposes to apply its minimization procedures to MCTs. See Aug. 30 Submission at 8-11.<sup>45</sup> Before discussing the measures proposed by the government for handling MCTs, it is helpful to begin with a brief overview of the NSA minimization procedures themselves. The procedures require that all acquisitions “will be conducted in a manner designed, to the greatest extent feasible, to minimize the acquisition of information not relevant to the authorized purpose of the collection.” NSA

---

<sup>45</sup> Although NSA has been collecting MCTs since before the Court’s approval of the first Section 702 certification in 2008, see June 1 Submission at 2, it has not, to date, applied the measures proposed here to the fruits of its upstream collection. Indeed, until NSA’s manual review of a six-month sample of its upstream collection revealed the acquisition of wholly domestic communications, the government asserted that NSA had never found a wholly domestic communication in its upstream collection. See id.

Minimization Procedures § 3(a).<sup>46</sup> Following acquisition, the procedures require that, “[a]s a communication is reviewed, NSA analyst(s) will determine whether it is a domestic or foreign communication to, from, or about a target and is reasonably believed to contain foreign intelligence information or evidence of a crime.” Id. § 3(b)(4). “Foreign communication means a communication that has at least one communicant outside of the United States.” Id. § 2(e). “All other communications, including communications in which the sender and all intended recipients are reasonably believed to be located in the United States at the time of acquisition, are domestic communications.” Id. In addition, domestic communications include “[a]ny communications acquired through the targeting of a person who at the time of targeting was reasonably believed to be located outside the United States but is in fact located inside the United States at the time such communications were acquired, and any communications acquired by targeting a person who at the time of the targeting was believed to be a non-United States person but was in fact a United States person . . . .” Id. § 3(d)(2). A domestic communication must be “promptly destroyed upon recognition unless the Director (or Acting Director) of NSA specifically determines, in writing, that” the communication contains foreign intelligence

---

<sup>46</sup> Of course, NSA’s separate targeting procedures, discussed above, also govern the manner in which communications are acquired.

information or evidence of a crime, or that it falls into another narrow exception permitting retention. See *id.* § 5.<sup>47</sup>

Upon determining that a communication is a "foreign communication," NSA must decide whether the communication is "of" or "concerning" a United States person. *Id.* § 6.

"Communications of a United States person include all communications to which a United States person is a party." *Id.* § 2(c). "Communications concerning a United States person include all communications in which a United States person is discussed or mentioned, except where such communications reveal only publicly-available information about the person." *Id.* § 2(b).

A foreign communication that is of or concerning a United States person and that is determined to contain neither foreign intelligence information nor evidence of a crime must be destroyed "at the earliest practicable point in the processing cycle," and "may be retained no longer than five years from the expiration date of the certification in any event." *Id.* § 3(b)(1).<sup>48</sup>

---

<sup>47</sup> Once such a determination is made by the Director, the domestic communications at issue are effectively treated as "foreign communications" for purposes of the rules regarding retention and dissemination.

<sup>48</sup> Although Section 3(b)(1) by its terms applies only to "inadvertently acquired communications of or concerning a United States person," the government has informed the Court that this provision is intended to apply, and in practice is applied, to all foreign communications of or concerning United States persons that contain neither foreign intelligence information nor evidence of a crime. Docket No. 702(i)-08-01, Sept. 2, 2008 Notice of Clarification and Correction at 3-5. Moreover, Section 3(c) of the procedures separately provides that foreign communications that do not qualify for retention and that "are known to contain communications of or concerning United States persons will be destroyed upon recognition," and, like unreviewed communications, "may be retained no longer than five years from the

(continued...)



A foreign communication that is of or concerning a United States person may be retained indefinitely if the “dissemination of such communications with reference to such United States persons would be permitted” under the dissemination provisions that are discussed below, or if it contains evidence of a crime. Id. § 6(a)(2)-(3). If the retention of a foreign communication of or concerning a United States person is “necessary for the maintenance of technical databases,” it may be retained for five years to allow for technical exploitation, or for longer than five years if more time is required for decryption or if the NSA Signals Intelligence Director “determines in writing that retention for a longer period is required to respond to authorized foreign intelligence or counterintelligence requirements.” Id. § 6(a)(1).

As a general rule, “[a] report based on communications of or concerning a United States person may be disseminated” only “if the identity of the United States person is deleted and a generic term or symbol is substituted so that the information cannot reasonably be connected with an identifiable United States person.” Id. § 6(b). A report including the identity of the United States person may be provided to a “recipient requiring the identity of such person for the performance of official duties,” but only if at least one of eight requirements is also met – for instance, if “the identity of the United States person is necessary to understand foreign intelligence information or assess its importance,” or if “information indicates the United States

---

<sup>48</sup>(...continued)  
expiration date of the certification authorizing the collection in any event.”

~~TOP SECRET//COMINT//ORCON,NOFORN~~

person may be . . . an agent of a foreign power” or that he is “engaging in international terrorism activities.” Id.<sup>49</sup>

*b. Proposed Minimization Measures for MCTs*

The government proposes that NSA’s minimization procedures be applied to MCTs in the following manner. After acquisition, upstream acquisitions, including MCTs, will reside in NSA repositories until they are accessed (e.g., in response to a query) by an NSA analyst performing his or her day-to-day work. NSA proposes adding a “cautionary banner” to the tools its analysts use to view the content of communications acquired through upstream collection under Section 702. See Aug. 30 Submission at 9. The banner, which will be “broadly displayed on [such] tools,” will “direct analysts to consult guidance on how to identify MCTs and how to handle them.” Id. at 9 & n.6.<sup>50</sup> Analysts will be trained to identify MCTs and to recognize wholly domestic communications contained within MCTs. See id. at 8-9.

When an analyst identifies an upstream acquisition as an MCT, the analyst will decide whether or not he or she “seek[s] to use a discrete communication within [the] MCT,”

---

<sup>49</sup> The procedures also permit NSA to provide unminimized communications to [REDACTED] FBI (subject to their own minimization procedures), and to foreign governments for the limited purpose of obtaining “technical and linguistic assistance.” NSA Minimization Procedures §§ 6(c), 8(b). Neither of these provisions has been used to share upstream acquisitions. Sept. 7, 2011 Hearing Tr. at 61-62.

<sup>50</sup> The banner will not be displayed for communications that “can be first identified through technical means where the active user is NSA’s tasked selector or that contain only a single, discrete communication based on particular stable and well-known protocols.” Aug. 30 Submission at 9 n.6. See infra, note 27, and supra, note 54.

~~TOP SECRET//COMINT//ORCON,NOFORN~~

presumably by reviewing some or all of the MCT's contents. Id. at 8.<sup>51</sup> "NSA analysts seeking to use a discrete communication contained in an MCT (for example, in a FISA application, intelligence report, or Section 702 targeting) will assess whether the discrete communication is to, from, or about a tasked selector." Id. The following framework will then be applied:

- If the discrete communication that the analyst seeks to use is to, from, or about a tasked selector, "any U.S. person information in that communication will be handled in accordance with the NSA minimization procedures." Id. Presumably, this means that the discrete communication will be treated as a "foreign communication" that is "of" or "concerning" a United States person, as described above. The MCT containing that communication remains available to analysts in NSA's repositories without any marking to indicate that it has been identified as an MCT or as a transaction containing United States person information.
- If the discrete communication sought to be used is not to, from, or about a tasked selector, and also not to or from an identifiable United States person, "that communication (including any U.S. person information therein) will be handled in accordance with the NSA minimization procedures." Id. at 8-9.<sup>52</sup> Presumably, this means that the discrete communication will be treated as a "foreign communication" or, if it contains information concerning a United States person, as a "foreign communication" "concerning a United States person," as described above. The MCT itself remains available to analysts in NSA's repositories without any marking to indicate that it has been identified as an MCT or that it contains one or more communications that are not to, from, or about a targeted selector.

---

<sup>51</sup> A transaction that is identified as an SCT rather than an MCT must be handled in accordance with the standard minimization procedures that are discussed above.

<sup>52</sup> The Court understands that absent contrary information, NSA treats the user of an account who appears to be located in the United States as "an identifiable U.S. person." See Aug. 30 Submission at 9 n.7 ("To help determine whether a discrete communication not to, from, or about a tasked selector is to or from a U.S. person, NSA would perform the same sort of technical analysis it would perform before tasking an electronic communications account/address/identifier in accordance with its section 702 targeting procedures.").

- A discrete communication that is not to, from, or about a tasked selector but that is to or from an identifiable United States person “cannot be used for any purpose other than to protect against an immediate threat to human life (e.g., force protection or hostage situations).” *Id.* at 9. Presumably, this is a reference to Section 1 of the minimization procedures, which allows NSA to deviate from the procedures in such narrow circumstances, subject to the requirement that prompt notice be given to the Office of the Director of National Intelligence, the Department of Justice, and the Court that the deviation has occurred. Regardless of whether or not the discrete communication is used for this limited purpose, the MCT itself remains in NSA’s databases without any marking to indicate that it is an MCT, or that it contains at least one communication that is to or from an identifiable United States person. *See id.*; Sept. 7, 2011 Hearing Tr. at 61.
- If the discrete communication sought to be used by the analyst (or another discrete communication within the MCT) is recognized as being wholly domestic, the entire MCT will be purged from NSA’s systems. *See* Aug. 30 Submission at 3.

*c. Statutory Analysis*

*i. Acquisition*

The Court first considers how NSA’s proposed handling of MCTs bears on whether NSA’s minimization procedures are “reasonably designed in light of the purpose and technique of the particular surveillance, to minimize the acquisition . . . of nonpublicly available information concerning unconsenting United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information.” *See* 50 U.S.C. § 1801(h)(1) (emphasis added). Insofar as NSA likely acquires approximately 2,000-10,000 MCTs each year that contain at least one wholly domestic communication that is neither to, from, nor about a targeted selector,<sup>53</sup> and tens of thousands of communications of or

---

<sup>53</sup> As noted above, NSA’s upstream collection also likely results in the acquisition of tens  
(continued...)

~~TOP SECRET//COMINT//ORCON,NOFORN~~

concerning United States persons with no direct connection to any target, the Court has serious concerns. The acquisition of such non-target communications, which are highly unlikely to have foreign intelligence value, obviously does not by itself serve the government's need to "obtain, produce, and disseminate foreign intelligence information." See 50 U.S.C. § 1801(h)(1).

The government submits, however, that the portions of MCTs that contain references to targeted selectors are likely to contain foreign intelligence information, and that it is not feasible for NSA to limit its collection only to the relevant portion or portions of each MCT – i.e., the particular discrete communications that are to, from, or about a targeted selector. The Court

---

<sup>53</sup>(...continued)

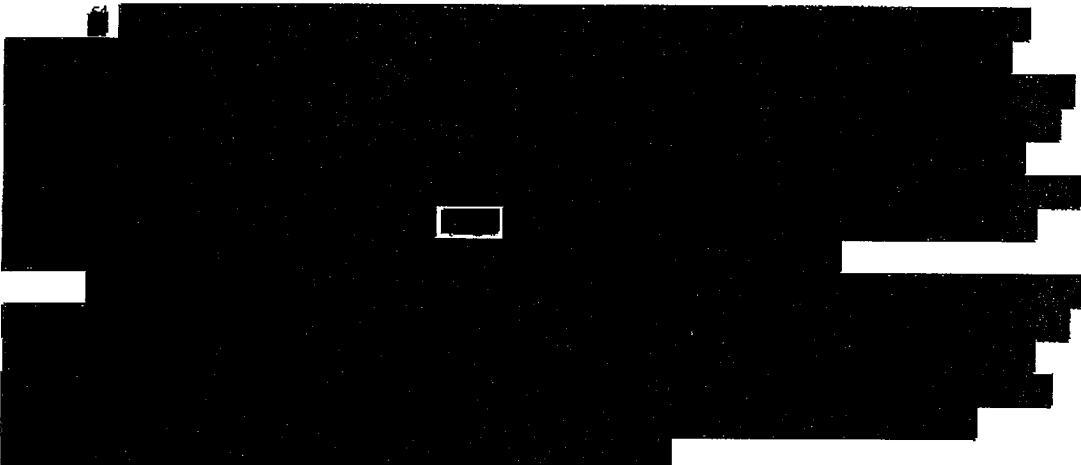
of thousands of wholly domestic SCTs that contain references to targeted selectors. See supra, pages 33-34 & note 33 (discussing the limits [REDACTED] [REDACTED])

Although the collection of wholly domestic "about" SCTs is troubling, they do not raise the same minimization-related concerns as discrete, wholly domestic communications that are neither to, from, nor about targeted selectors, or as discrete communications of or concerning United States persons with no direct connection to any target, either of which may be contained within MCTs. The Court has effectively concluded that certain communications containing a reference to a targeted selector are reasonably likely to contain foreign intelligence information, including communications between non-target accounts that contain the name of the targeted facility in the body of the message. See Docket No. 07-449, May 31, 2007 Primary Order at 12 (finding probable cause to believe that certain "about" communications were "themselves being sent and/or received by one of the targeted foreign powers"). Insofar as the discrete, wholly domestic "about" communications at issue here are communications between non-target accounts that contain the name of the targeted facility, the same conclusion applies to them. Accordingly, in the language of FISA's definition of minimization procedures, the acquisition of wholly domestic communications about targeted selectors will generally be "consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information." See 50 U.S.C. 1801(h)(1). Nevertheless, the Court understands that in the event NSA identifies a discrete, wholly domestic "about" communication in its databases, the communication will be destroyed upon recognition. See NSA Minimization Procedures § 5.

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

accepts the government's assertion that the collection of MCTs yields valuable foreign intelligence information that by its nature cannot be acquired except through upstream collection. See Sept. 7, 2011 Hearing Tr. at 69-70, 74. For purposes of this discussion, the Court further accepts the government's assertion that it is not feasible for NSA to avoid the collection of MCTs as part of its upstream collection or to limit its collection only to the specific portion or portions of each transaction that contains the targeted selector. See id. at 48-50; June 1 Submission at 27.<sup>54</sup> The Court therefore concludes that NSA's minimization procedures are, given the current state of NSA's technical capability, reasonably designed to minimize the acquisition of nonpublicly available information concerning unconsenting United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information.



In any event, it is incumbent upon NSA to continue working to enhance its capability to limit acquisitions only to targeted communications.

~~TOP SECRET//COMINT//ORCON,NOFORN~~

*ii. Retention*

The principal problem with the government's proposed handling of MCTs relates to what will occur, and what will not occur, following acquisition. As noted above, the NSA minimization procedures generally require that, "[a]s a communication is reviewed, NSA analyst(s) will determine whether it is a domestic or foreign communication to, from, or about a target and is reasonably believed to contain foreign intelligence information or evidence of a crime," see NSA Minimization Procedures § 3(b)(4), so that it can be promptly afforded the appropriate treatment under the procedures. The measures proposed by the government for MCTs, however, largely dispense with the requirement of prompt disposition upon initial review by an analyst. Rather than attempting to identify and segregate information "not relevant to the authorized purpose of the acquisition" or to destroy such information promptly following acquisition, NSA's proposed handling of MCTs tends to maximize the retention of such information, including information of or concerning United States persons with no direct connection to any target. See id. § 3(b)(1).

The proposed measures focus almost exclusively on the discrete communications within MCTs that analysts decide, after review, that they wish to use. See Aug. 30 Submission at 8-10. An analyst is not obligated to do anything with other portions of the MCT, including any wholly domestic discrete communications that are not immediately recognized as such, and communications of or concerning United States persons that have no direct connection to the targeted selector. See id.; Sept. 7, 2011 Hearing Tr. at 61. If, after reviewing the contents of an

entire MCT, the analyst decides that he or she does not wish to use any discrete communication contained therein, the analyst is not obligated to do anything unless it is immediately apparent to him or her that the MCT contains a wholly domestic communication (in which case the entire MCT is deleted).<sup>55</sup> See Aug. 30 Submission at 8-10.

Except in the case of those recognized as containing at least one wholly domestic communication, MCTs that have been reviewed by analysts remain available to other analysts in NSA's repositories without any marking to identify them as MCTs. See id.; Sept. 7, 2011 Hearing Tr. at 61. Nor will MCTs be marked to identify them as containing discrete communications to or from United States persons but not to or from a targeted selector, or to indicate that they contain United States person information. See Aug. 30 Submission at 8-10; Sept. 7, 2011 Hearing Tr. at 61. All MCTs except those identified as containing one or more wholly domestic communications will be retained for a minimum of five years. The net effect is that thousands of wholly domestic communications (those that are never reviewed and those that are not recognized by analysts as being wholly domestic), and thousands of other discrete

---

<sup>55</sup> The government's submissions make clear that, in many cases, it will be difficult for analysts to determine whether a discrete communication contained within an MCT is a wholly domestic communication. NSA's recent manual review of a six-month representative sample of its upstream collection demonstrates how challenging it can be for NSA to recognize wholly domestic communications, even when the agency's full attention and effort are directed at the task. See generally Aug. 16 and Aug. 30 Submissions. It is doubtful that analysts whose attention and effort are focused on identifying and analyzing foreign intelligence information will be any more successful in identifying wholly domestic communications. Indeed, each year the government notifies the Court of numerous compliance incidents involving good-faith mistakes and omissions by NSA personnel who work with the Section 702 collection.



communications that are not to or from a targeted selector but that are to, from, or concerning a United States person, will be retained by NSA for at least five years, despite the fact that they have no direct connection to a targeted selector and, therefore, are unlikely to contain foreign intelligence information.

It appears that NSA could do substantially more to minimize the retention of information concerning United States persons that is unrelated to the foreign intelligence purpose of its upstream collection. The government has not, for instance, demonstrated why it would not be feasible to limit access to upstream acquisitions to a smaller group of specially-trained analysts who could develop expertise in identifying and scrutinizing MCTs for wholly domestic communications and other discrete communications of or concerning United States persons. Alternatively, it is unclear why an analyst working within the framework proposed by the government should not be required, after identifying an MCT, to apply Section 3(b)(4) of the NSA minimization procedures to each discrete communication within the transaction. As noted above, Section 3(b)(4) states that “[a]s a communication is reviewed, NSA analyst(s) will determine whether it is a domestic or foreign communication to, from, or about a target and is reasonably believed to contain foreign intelligence information or evidence of a crime.” NSA Minimization Procedures § 3(b)(4). If the MCT contains information “of” or “concerning” a United States person within the meaning of Sections (2)(b) and (2)(c) of the NSA minimization procedures, it is unclear why the analyst should not be required to mark it to identify it as such. At a minimum, it seems that the entire MCT could be marked as an MCT. Such markings would

alert other NSA personnel who might encounter the MCT to take care in reviewing it, thus reducing the risk of error that seems to be inherent in the measures proposed by the government, which are applied by each analyst, acting alone and without the benefit of his or her colleagues' prior efforts.<sup>56</sup> Another potentially helpful step might be to adopt a shorter retention period for MCTs and unreviewed upstream communications so that such information "ages off" and is deleted from NSA's repositories in less than five years.

This discussion is not intended to provide a checklist of changes that, if made, would necessarily bring NSA's minimization procedures into compliance with the statute. Indeed, it may be that some of these measures are impracticable, and it may be that there are other plausible (perhaps even better) steps that could be taken that are not mentioned here. But by not fully exploring such options, the government has failed to demonstrate that it has struck a reasonable balance between its foreign intelligence needs and the requirement that information concerning United States persons be protected. Under the circumstances, the Court is unable to find that, as applied to MCTs in the manner proposed by the government, NSA's minimization procedures are "reasonably designed in light of the purpose and technique of the particular surveillance to minimize the . . . retention . . . of nonpublicly available information concerning unconsenting

---

<sup>56</sup> The government recently acknowledged that "it's pretty clear that it would be better" if NSA used such markings but that "[t]he feasibility of doing that [had not yet been] assessed." Sept. 7, 2011 Hearing Tr. at 56.

~~TOP SECRET//COMINT//ORCON,NOFORN~~

United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information.”<sup>57</sup> See 50 U.S.C. §§ 1801(h)(1) & 1821(4)(A).

*iii. Dissemination*

The Court next turns to dissemination. At the outset, it must be noted that FISA imposes a stricter standard for dissemination than for acquisition or retention. While the statute requires procedures that are reasonably designed to “minimize” the acquisition and retention of information concerning United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information, the procedures must be reasonably designed to “prohibit” the dissemination of information concerning United States persons consistent with that need. See 50 U.S.C. § 1801(h)(1) (emphasis added).

---

<sup>57</sup> NSA’s minimization procedures contain two provisions that state, in part, that “[t]he communications that may be retained [by NSA] include electronic communications acquired because of limitations

[REDACTED]. The government further represented that it “ha[d] not seen” such a circumstance in collection under the Protect America Act (“PAA”), which was the predecessor to Section 702. *Id.* at 29, 30. And although NSA apparently was acquiring Internet transactions under the PAA, the government made no mention of such acquisitions in connection with these provisions of the minimization procedures (or otherwise). See *id.* at 27-31. Accordingly, the Court does not read this language as purporting to justify the procedures proposed by the government for MCTs. In any event, such a reading would, for the reasons stated, be inconsistent with the statutory requirements for minimization.

~~TOP SECRET//COMINT//ORCON,NOFORN~~

As the Court understands it, no United States-person-identifying information contained in any MCT will be disseminated except in accordance with the general requirements of NSA's minimization procedures for "foreign communications" "of or concerning United States persons" that are discussed above. Specifically, "[a] report based on communications of or concerning a United States person may be disseminated" only "if the identity of the United States person is deleted and a generic term or symbol is substituted so that the information cannot reasonably be connected with an identifiable United States person." NSA Minimization Procedures § 6(b). A report including the identity of the United States person may be provided to a "recipient requiring the identity of such person for the performance of official duties," but only if at least one of eight requirements is also met – for instance, if "the identity of the United States person is necessary to understand foreign intelligence information or assess its importance." *Id.*<sup>58</sup>

This limitation on the dissemination of United States-person-identifying information is helpful. But the pertinent portion of FISA's definition of minimization procedures applies not merely to information that identifies United States persons, but more broadly to the dissemination of "information concerning unconsenting United States persons." 50 U.S.C. § 1801(h)(1) (emphasis added).<sup>59</sup> The government has proposed several additional restrictions that

---

<sup>58</sup> Although Section 6(b) uses the term "report," the Court understands it to apply to the dissemination of United States-person-identifying information in any form.

<sup>59</sup> Another provision of the definition of minimization procedures bars the dissemination of information (other than certain forms of foreign intelligence information) "in a manner that  
(continued...)"

will have the effect of limiting the dissemination of “nonpublicly available information concerning unconsenting United States persons consistent with the need of the United States to disseminate foreign intelligence information.” *Id.* First, as noted above, the government will destroy MCT’s that are recognized by analysts as containing one or more discrete wholly domestic communications. Second, the government has asserted that NSA will not use any discrete communication within an MCT that is determined to be to or from a United States person but not to, from, or about a targeted selector, except when necessary to protect against an immediate threat to human life. *See* Aug. 30 Submission at 9. The Court understands this to mean, among other things, that no information from such a communication will be disseminated in any form unless NSA determines it is necessary to serve this specific purpose. Third, the government has represented that whenever it is unable to confirm that at least one party to a discrete communication contained in an MCT is located outside the United States, it will not use any information contained in the discrete communication. *See* Sept. 7, 2011 Hearing Tr. at 52. The Court understands this limitation to mean that no information from such a discrete communication will be disseminated by NSA in any form.

Communications as to which a United States person or a person inside the United States

---

<sup>59</sup>(...continued)

identifies any United States person,” except when the person’s identity is necessary to understand foreign intelligence information or to assess its importance. *See* 50 U.S.C. §§ 1801(h)(2), 1821(4)(b). Congress’s use of the distinct modifying terms “concerning” and “identifying” in two adjacent and closely-related provisions was presumably intended to have meaning. *See, e.g., Russello v. United States*, 464 U.S. 16, 23 (1983).

is a party are more likely than other communications to contain information concerning United States persons. And when such a communication is neither to, from, nor about a targeted facility, it is highly unlikely that the “need of the United States to disseminate foreign intelligence information” would be served by the dissemination of United States-person information contained therein. Hence, taken together, these measures will tend to prohibit the dissemination of information concerning unconsenting United States persons when there is no foreign-intelligence need to do so.<sup>60</sup> Of course, the risk remains that information concerning United States persons will not be recognized by NSA despite the good-faith application of the measures it proposes. But the Court cannot say that the risk is so great that it undermines the reasonableness of the measures proposed by NSA with respect to the dissemination of information concerning United States persons.<sup>61</sup> Accordingly, the Court concludes that NSA’s

---

<sup>60</sup> Another measure that, on balance, is likely to mitigate somewhat the risk that information concerning United States persons will be disseminated in the absence of a foreign-intelligence need is the recently-proposed prohibition on running queries of the Section 702 upstream collection using United States-person identifiers. See Aug. 30 Submission at 10-11. To be sure, any query, including a query based on non-United States-person information, could yield United States-person information. Nevertheless, it stands to reason that queries based on information concerning United States persons are at least somewhat more likely than other queries to yield United States-person information. Insofar as information concerning United States persons is not made available to analysts, it cannot be disseminated. Of course, this querying restriction does not address the retention problem that is discussed above.

<sup>61</sup> In reaching this conclusion regarding the risk that information concerning United States persons might be mistakenly disseminated, the Court is mindful that by taking additional steps to minimize the retention of such information, NSA would also be reducing the likelihood that it might be disseminated when the government has no foreign intelligence need to do so.

~~TOP SECRET//COMINT//ORCON,NOFORN~~

minimization procedures are reasonably designed to “prohibit the dissemination[] of nonpublicly available information concerning unconsenting United States persons consistent with the need of the United States to . . . disseminate foreign intelligence information.” See 50 U.S.C.

§ 1801(h)(1).<sup>62</sup>

4. NSA’S Targeting and Minimization Procedures Do Not, as Applied to Upstream Collection that Includes MCTs, Satisfy the Requirements of the Fourth Amendment.

The final question for the Court is whether the targeting and minimization procedures are, as applied to upstream collection that includes MCTs, consistent with the Fourth Amendment.

See 50 U.S.C. § 1881a(i)(3)(A)-(B). The Fourth Amendment provides:

The 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.

The Court has assumed in the prior Section 702 Dockets that at least in some circumstances, account holders have a reasonable expectation of privacy in electronic communications, and hence that the acquisition of such communications can result in a “search” or “seizure” within the meaning of the Fourth Amendment. See, e.g., Docket No. [REDACTED]

[REDACTED]. The government accepts the proposition that the acquisition of

---

<sup>62</sup> The Court further concludes that the NSA minimization procedures, as the government proposes to apply them to MCTs, satisfy the requirements of 50 U.S.C. §§ 1801(h)(2)-(3) and 1821(4)(B)-(C). See supra, note 59 (discussing 50 U.S.C. §§ 1801(h)(2) & 1821(4)(B)). The requirements of 50 U.S.C. §§ 1801(h)(4) and 1821(4)(D) are inapplicable here.

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

electronic communications can result in a “search” or “seizure” under the Fourth Amendment. See Sept. 7, 2011 Hearing Tr. at 66. Indeed, the government has acknowledged in prior Section 702 matters that the acquisition of communications from facilities used by United States persons located outside the United States “must be in conformity with the Fourth Amendment.” Docket Nos. [REDACTED]. The same is true of the acquisition of communications from facilities used by United States persons and others within the United States. See United States v. Verdugo-Urquidez, 494 U.S. 259, 271 (1990) (recognizing that “aliens receive constitutional protections when they have come within the territory of the United States and developed substantial connections with this country”).

*a. The Warrant Requirement*

The Court has previously concluded that the acquisition of foreign intelligence information pursuant to Section 702 falls within the “foreign intelligence exception” to the warrant requirement of the Fourth Amendment. See Docket No. [REDACTED]. The government’s recent revelations regarding NSA’s acquisition of MCTs do not alter that conclusion. To be sure, the Court now understands that, as a result of the transactional nature of the upstream collection, NSA acquires a substantially larger number of communications of or concerning United States persons and persons inside the United States than previously understood. Nevertheless, the collection as a whole is still directed at [REDACTED] [REDACTED] [REDACTED] conducted for the purpose of national security – a

~~TOP SECRET//COMINT//ORCON,NOFORN~~



purpose going “well beyond any garden-variety law enforcement objective.” See *id.* (quoting *In re Directives*, Docket No. 08-01, Opinion at 16 (FISA Ct. Rev. Aug. 22, 2008) (hereinafter “*In re Directives*”).<sup>63</sup> Further, it remains true that the collection is undertaken in circumstances in which there is a “high degree of probability that requiring a warrant would hinder the government’s ability to collect time-sensitive information and, thus, would impede the vital national security interests that are at stake.” *Id.* at 36 (quoting *In re Directives* at 18). Accordingly, the government’s revelation that NSA acquires MCTs as part of its Section 702 upstream collection does not disturb the Court’s prior conclusion that the government is not required to obtain a warrant before conducting acquisitions under NSA’s targeting and minimization procedures.

*b. Reasonableness*

The question therefore becomes whether, taking into account NSA’s acquisition and proposed handling of MCTs, the agency’s targeting and minimization procedures are reasonable under the Fourth Amendment. As the Foreign Intelligence Surveillance Court of Review (“Court of Review”) has explained, a court assessing reasonableness in this context must consider “the nature of the government intrusion and how the government intrusion is implemented. The more important the government’s interest, the greater the intrusion that may be constitutionally

---

<sup>63</sup> A redacted, de-classified version of the opinion in *In re Directives* is published at 551 F.3d 1004. The citations herein are to the unredacted, classified version of the opinion.

~~TOP SECRET//COMINT//ORCON,NOFORN~~

tolerated.” In re Directives at 19-20 (citations omitted), quoted in Docket No. [REDACTED]

[REDACTED]. The court must therefore

balance the interests at stake. If the protections that are in place for individual privacy interests are sufficient in light of the government interest at stake, the constitutional scales will tilt in favor of upholding the government’s actions. If, however, those protections are insufficient to alleviate the risks of government error and abuse, the scales will tip toward a finding of unconstitutionality.

Id. at 20 (citations omitted), quoted in Docket No. [REDACTED].

In conducting this balancing, the Court must consider the “totality of the circumstances.” Id. at 19. Given the all-encompassing nature of Fourth Amendment reasonableness review, the targeting and minimization procedures are most appropriately considered collectively. See Docket No. [REDACTED] (following the same approach).<sup>64</sup>

The Court has previously recognized that the government’s national security interest in conducting acquisitions pursuant to Section 702 “is of the highest order of magnitude.” Docket No. [REDACTED] (quoting In re Directives at 20). The Court has further accepted the government’s representations that NSA’s upstream collection is “uniquely capable of acquiring certain types of targeted communications containing valuable foreign intelligence information.” Docket No. [REDACTED] (quoting

---

<sup>64</sup> Reasonableness review under the Fourth Amendment is broader than the statutory assessment previously addressed, which is necessarily limited by the terms of the pertinent provisions of FISA.

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

government filing). There is no reason to believe that the collection of MCTs results in the acquisition of less foreign intelligence information than the Court previously understood.

Nevertheless, it must be noted that NSA's upstream collection makes up only a very small fraction of the agency's total collection pursuant to Section 702. As explained above, the collection of telephone communications under Section 702 is not implicated at all by the government's recent disclosures regarding NSA's acquisition of MCTs. Nor do those disclosures affect NSA's collection of Internet communications directly from Internet service providers [REDACTED], which accounts for approximately 91% of the Internet communications acquired by NSA each year under Section 702. See Aug. 16 Submission at Appendix A. And the government recently advised that NSA now has the capability, at the time of acquisition, to identify approximately 40% of its upstream collection as constituting discrete communications (non-MCTs) that are to, from, or about a targeted selector. See id. at 1 n.2. Accordingly, only approximately 5.4% (40% of 9%) of NSA's aggregate collection of Internet communications (and an even smaller portion of the total collection) under Section 702 is at issue here. The national security interest at stake must be assessed bearing these numbers in mind.

The government's recent disclosures regarding the acquisition of MCTs most directly affect the privacy side of the Fourth Amendment balance. The Court's prior approvals of the targeting and minimization procedures rested on its conclusion that the procedures "reasonably confine acquisitions to targets who are non-U.S. persons outside the United States," who thus

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

“are not protected by the Fourth Amendment.” Docket No [REDACTED]

[REDACTED] The Court’s approvals also rested upon the understanding that acquisitions under the procedures “will intrude on interests protected by the Fourth Amendment only to the extent that (1) despite the operation of the targeting procedures, U.S. persons, or persons actually in the United States, are mistakenly targeted; or (2) U.S. persons, or persons located in the United States, are parties to communications to or from tasked selectors (or, in certain circumstances, communications that contain a reference to a tasked selector).” *Id.* at 38. But NSA’s acquisition of MCTs substantially broadens the circumstances in which Fourth Amendment-protected interests are intruded upon by NSA’s Section 702 collection. Until now, the Court has not considered these acquisitions in its Fourth Amendment analysis.

Both in terms of its size and its nature, the intrusion resulting from NSA’s acquisition of MCTs is substantial. The Court now understands that each year, NSA’s upstream collection likely results in the acquisition of roughly two to ten thousand discrete wholly domestic communications that are neither to, from, nor about a targeted selector, as well as tens of thousands of other communications that are to or from a United States person or a person in the United States but that are neither to, from, nor about a targeted selector.<sup>65</sup> In arguing that NSA’s

---

<sup>65</sup> As discussed earlier, NSA also likely acquires tens of thousands of discrete, wholly domestic communications that are “about” a targeted facility. Because these communications are reasonably likely to contain foreign intelligence information and thus, generally speaking, serve the government’s foreign intelligence needs, they do not present the same Fourth Amendment concerns as the non-target communications discussed here. *See supra*, note 53.

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

targeting and minimization procedures satisfy the Fourth Amendment notwithstanding the acquisition of MCTs, the government stresses that the number of protected communications acquired is relatively small in comparison to the total number of Internet communications obtained by NSA through its upstream collection. That is true enough, given the enormous volume of Internet transactions acquired by NSA through its upstream collection (approximately 26.5 million annually). But the number is small only in that relative sense. The Court recognizes that the ratio of non-target, Fourth Amendment-protected communications to the total number of communications must be considered in the Fourth Amendment balancing. But in conducting a review under the Constitution that requires consideration of the totality of the circumstances, see In re Directives at 19, the Court must also take into account the absolute number of non-target, protected communications that are acquired. In absolute terms, tens of thousands of non-target, protected communications annually is a very large number.

The nature of the intrusion at issue is also an important consideration in the Fourth Amendment balancing. See, e.g., Board of Educ. v. Earls, 536 U.S. 822, 832 (2002); Vernonia Sch. Dist. 47J v. Acton, 515 U.S. 646, 659 (1995). At issue here are the personal [REDACTED] communications of U.S. persons and persons in the United States. A person's "papers" are among the four items that are specifically listed in the Fourth Amendment as subject to protection against unreasonable search and seizure. Whether they are transmitted by letter,

~~TOP SECRET//COMINT//ORCON,NOFORN~~

telephone or e-mail, a person's private communications are akin to personal papers. Indeed, the Supreme Court has held that the parties to telephone communications and the senders and recipients of written communications generally have a reasonable expectation of privacy in the contents of those communications. See Katz, 389 U.S. at 352; United States v. United States Dist. Ct. (Keith), 407 U.S. 297, 313 (1972); United States v. Jacobsen, 466 U.S. 109, 114 (1984). The intrusion resulting from the interception of the contents of electronic communications is, generally speaking, no less substantial.<sup>66</sup>

The government stresses that the non-target communications of concern here (discrete wholly domestic communications and other discrete communications to or from a United States person or a person in the United States that are neither to, from, nor about a targeted selector) are acquired incidentally rather than purposefully. See June 28 Submission at 13-14. Insofar as NSA acquires entire MCTs because it lacks the technical means to limit collection only to the discrete portion or portions of each MCT that contain a reference to the targeted selector, the Court is satisfied that is the case. But as the government correctly recognizes, the acquisition of non-target information is not necessarily reasonable under the Fourth Amendment simply

---

<sup>66</sup> Of course, not every interception by the government of a personal communication results in a "search" or "seizure" within the meaning of the Fourth Amendment. Whether a particular intrusion constitutes a search or seizure depends on the specific facts and circumstances involved.

~~TOP SECRET//COMINT//ORCON,NOFORN~~

because its collection is incidental to the purpose of the search or surveillance. See id. at 14.

There surely are circumstances in which incidental intrusions can be so substantial as to render a search or seizure unreasonable. To use an extreme example, if the only way for the government to obtain communications to or from a particular targeted ██████████ required also acquiring all communications to or from every other ██████████, such collection would certainly raise very serious Fourth Amendment concerns.

Here, the quantity and nature of the information that is “incidentally” collected distinguishes this matter from the prior instances in which this Court and the Court of Review have considered incidental acquisitions. As explained above, the quantity of incidentally-acquired, non-target, protected communications being acquired by NSA through its upstream collection is, in absolute terms, very large, and the resulting intrusion is, in each instance, likewise very substantial. And with regard to the nature of the acquisition, the government acknowledged in a prior Section 702 docket that the term “incidental interception” is “most commonly understood to refer to an intercepted communication between a target using a facility subject to surveillance and a third party using a facility not subject to surveillance.” Docket Nos. ██████████ This is the sort of acquisition that the Court of Review was addressing in In re Directives when it stated that “incidental collections occurring as a result of constitutionally permissible acquisitions do not

~~TOP SECRET//COMINT//ORCON,NOFORN~~

render those acquisitions unlawful.” In re Directives at 30. But here, by contrast, the incidental acquisitions of concern are not direct communications between a non-target third party and the user of the targeted facility. Nor are they the communications of non-targets that refer directly to a targeted selector. Rather, the communications of concern here are acquired simply because they appear somewhere in the same transaction as a separate communication that is to, from, or about the targeted facility.<sup>67</sup>

The distinction is significant and impacts the Fourth Amendment balancing. A discrete communication as to which the user of the targeted facility is a party or in which the targeted

---

<sup>67</sup> The Court of Review plainly limited its holding regarding incidental collection to the facts before it. See In re Directives at 30 (“On these facts, incidentally collected communications of non-targeted United States persons do not violate the Fourth Amendment.”) (emphasis added). The dispute in In re Directives involved the acquisition by NSA of discrete to/from communications from an Internet Service Provider, not NSA’s upstream collection of Internet transactions. Accordingly, the Court of Review had no occasion to consider NSA’s acquisition of MCTs (or even “about” communications, for that matter). Furthermore, the Court of Review noted that “[t]he government assures us that it does not maintain a database of incidentally collected information from non-targeted United States persons, and there is no evidence to the contrary.” Id. Here, however, the government proposes measures that will allow NSA to retain non-target United States person information in its databases for at least five years.

The Title III cases cited by the government (see June 28 Submission at 14-15) are likewise distinguishable. Abraham v. County of Greenville, 237 F.3d 386, 391 (4th Cir. 2001), did not involve incidental overhears at all. The others involved allegedly non-pertinent communications to or from the facilities for which wiretap authorization had been granted, rather than communications to or from non-targeted facilities. See Scott v. United States, 436 U.S. 128, 130-31 (1978), United States v. McKinnon, 721 F.2d 19, 23 (1st Cir. 1983), and United States v. Doolittle, 507 F.2d 1368, 1371, *aff’d en banc*, 518 F.2d 500 (5th Cir. 1975).



~~TOP SECRET//COMINT//ORCON,NOFORN~~

facility is mentioned is much more likely to contain foreign intelligence information than is a separate communication that is acquired simply because it happens to be within the same transaction as a communication involving a targeted facility. Hence, the national security need for acquiring, retaining, and disseminating the former category of communications is greater than the justification for acquiring, retaining, and disseminating the latter form of communication.

The Court of Review and this Court have recognized that the procedures governing retention, use, and dissemination bear on the reasonableness under the Fourth Amendment of a program for collecting foreign intelligence information. See In re Directives at 29-30; Docket No. [REDACTED]. As explained in the discussion of NSA's minimization procedures above, the measures proposed by NSA for handling MCTs tend to maximize, rather than minimize, the retention of non-target information, including information of or concerning United States persons. Instead of requiring the prompt review and proper disposition of non-target information (to the extent it is feasible to do so), NSA's proposed measures focus almost exclusively on those portions of an MCT that an analyst decides, after review, that he or she wishes to use. An analyst is not required to determine whether other portions of the MCT constitute discrete communications to or from a United States person or a person in the United States, or contain information concerning a United States person or person inside the United States, or, having made such a determination, to do anything about it. Only

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

those MCTs that are immediately recognized as containing a wholly domestic discrete communication are purged, while other MCTs remain in NSA's repositories for five or more years, without being marked as MCTs. Nor, if an MCT contains a discrete communication of, or other information concerning, a United States person or person in the United States, is the MCT marked as such. Accordingly, each analyst who retrieves an MCT and wishes to use a portion thereof is left to apply the proposed minimization measures alone, from beginning to end, and without the benefit of his colleagues' prior review and analysis. Given the limited review of MCTs that is required, and the difficulty of the task of identifying protected information within an MCT, the government's proposed measures seem to enhance, rather than reduce, the risk of error, overretention, and dissemination of non-target information, including information protected by the Fourth Amendment.

In sum, NSA's collection of MCTs results in the acquisition of a very large number of Fourth Amendment-protected communications that have no direct connection to any targeted facility and thus do not serve the national security needs underlying the Section 702 collection as a whole. Rather than attempting to identify and segregate the non-target, Fourth-Amendment protected information promptly following acquisition, NSA's proposed handling of MCTs tends to maximize the retention of such information and hence to enhance the risk that it will be used and disseminated. Under the totality of the circumstances, then, the Court is unable to find that

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

the government's proposed application of NSA's targeting and minimization procedures to MCTs is consistent with the requirements of the Fourth Amendment. The Court does not foreclose the possibility that the government might be able to tailor the scope of NSA's upstream collection, or adopt more stringent post-acquisition safeguards, in a manner that would satisfy the reasonableness requirement of the Fourth Amendment.<sup>68</sup>

## V. CONCLUSION

For the foregoing reasons, the government's requests for approval of the certifications and procedures contained in the April 2011 Submissions are granted in part and denied in part. The Court concludes that one aspect of the proposed collection – the “upstream collection” of Internet transactions containing multiple communications, or MCTs – is, in some respects, deficient on statutory and constitutional grounds. Specifically, the Court finds as follows:

1. Certifications [REDACTED] and the amendments to the Certifications in the Prior 702 Dockets, contain all the required elements;

---

<sup>68</sup> As the government notes, *see* June 1 Submission at 18-19, the Supreme Court has “repeatedly refused to declare that only the ‘least intrusive’ search practicable can be reasonable under the Fourth Amendment.” *City of Ontario v. Quon*, — U.S. —, 130 S. Ct. 2619, 2632 (2010) (citations and internal quotation marks omitted). The foregoing discussion should not be understood to suggest otherwise. Rather, the Court holds only that the means actually chosen by the government to accomplish its Section 702 upstream collection are, with respect to MCTs, excessively intrusive in light of the purpose of the collection as a whole.

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

2. As applied to telephone communications and discrete Internet communications that are to or from a facility tasked for collection, to non-MCT "about" communications falling within the [REDACTED] categories previously described by the government,<sup>69</sup> and to MCTs as to which the "active user" is known to be a tasked selector, the targeting and minimization procedures adopted in accordance with 50 U.S.C. § 1881a(d)-(e) are consistent with the requirements of those subsections and with the Fourth Amendment to the Constitution of the United States;

3. NSA's targeting procedures, as the government proposes to implement them in connection with the acquisition of MCTs, meet the requirements of 50 U.S.C. § 1881a(d);

4. NSA's minimization procedures, as the government proposes to apply them to MCTs as to which the "active user" is not known to be a tasked selector, do not meet the requirements of 50 U.S.C. § 1881a(e) with respect to retention; and

5. NSA's targeting and minimization procedures, as the government proposes to apply them to MCTs as to which the "active user" is not known to be a tasked selector, are inconsistent with the requirements of the Fourth Amendment.

---

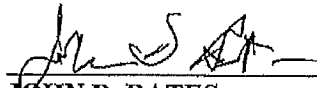
<sup>69</sup> See Docket No. [REDACTED]

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

Orders approving the certifications and amendments in part are being entered contemporaneously herewith.

ENTERED this 3rd day of October, 2011.



JOHN D. BATES  
Judge, United States Foreign  
Intelligence Surveillance Court

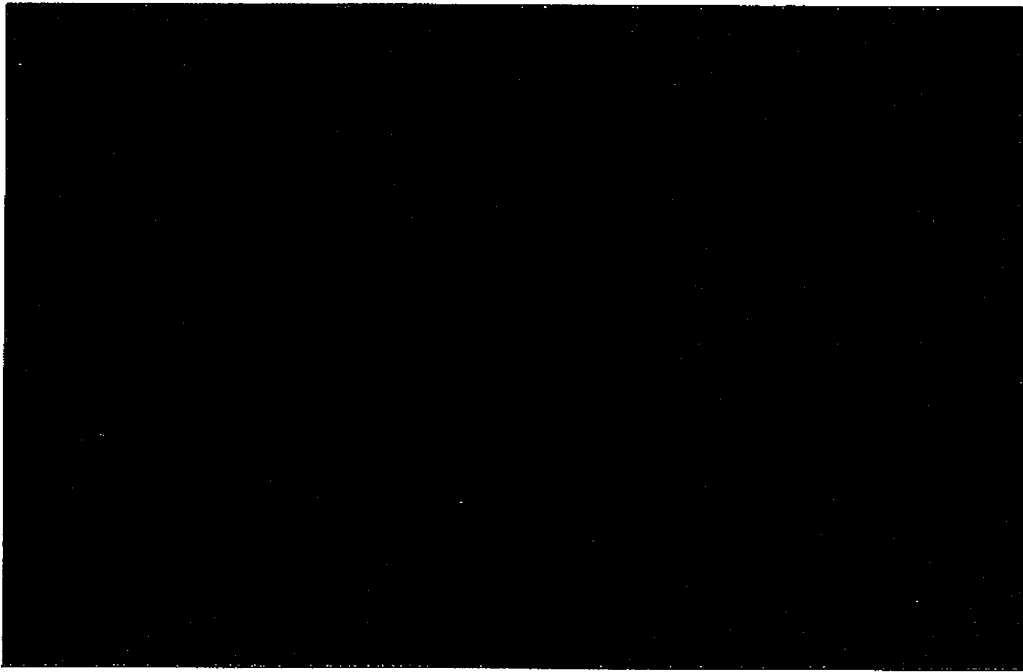
[Redacted], Deputy Clerk,  
FISC, certify that this document  
is a true and correct copy of  
the original. [Redacted]

~~TOP SECRET//COMINT//ORCON,NOFORN~~

(b)(6)

~~TOP SECRET//COMINT//ORCON,NOFORN~~

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



**ORDER**

These matters are before the Court on: (1) the "Government's Ex Parte Submission of Reauthorization Certification and Related Procedures, Ex Parte Submission of Amended Certifications, and Request for an Order Approving Such Certification and Amended Certifications" for DNI/AG 702(g) Certifications [REDACTED] which was filed

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

on April 20, 2011; (2) the "Government's Ex Parte Submission of Reauthorization Certification and Related Procedures, Ex Parte Submission of Amended Certifications, and Request for an Order Approving Such Certification and Amended Certifications" for DNI/AG 702(g) Certifications [REDACTED], which was filed on April 22, 2011; and (3) the "Government's Ex Parte Submission of Reauthorization Certification and Related Procedures, Ex Parte Submission of Amended Certifications, and Request for an Order Approving Such Certification and Amended Certifications" for DNI/AG 702(g) Certifications [REDACTED], which was also filed on April 22, 2011 (collectively, the "April 2011 Submissions").

Through the April 2011 Submissions, the government seeks approval of the acquisition of certain telephone and Internet communications pursuant to Section 702 of the Foreign Intelligence Surveillance Act ("FISA" or the "Act"), 50 U.S.C. § 1881a, which requires judicial review for compliance with both statutory and constitutional requirements. For the reasons set forth in the accompanying Memorandum Opinion, the government's requests for approval are granted in part and denied in part. The Court concludes that one aspect of the proposed collection – the "upstream collection" of Internet transactions containing multiple communications, or "MCTs" – is, in some respects, deficient on statutory and constitutional grounds. Specifically, the Court finds as follows:

1. DNI/AG 702(g) Certifications [REDACTED], as well as the amendments to the other certifications listed above and contained in the April 2011 Submissions,

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

contain all the required elements;

2. As applied to telephone communications and discrete Internet communications that are to or from a facility tasked for collection, to non-MCT "about" communications falling within the [REDACTED] categories previously described by the government,<sup>1</sup> and to MCTs as to which the "active user" is known to be a tasked selector, the targeting and minimization procedures adopted in accordance with 50 U.S.C. § 1881a(d)-(e) are consistent with the requirements of those subsections and with the Fourth Amendment to the Constitution of the United States;

3. NSA's targeting procedures, as the government proposes to implement them in connection with the acquisition of MCTs, meet the requirements of 50 U.S.C. § 1881a(d);

4. NSA's minimization procedures, as the government proposes to apply them to MCTs as to which the "active user" is not known to be a tasked selector, do not meet the requirements of 50 U.S.C. § 1881a(e) with respect to retention; and

5. NSA's targeting and minimization procedures, as the government proposes to apply them to MCTs as to which the "active user" is not known to be a tasked selector, are inconsistent with the requirements of the Fourth Amendment.

Accordingly, pursuant to 50 U.S.C. § 1881a(i)(3)(B), the government shall, at its election:

(a) not later than 30 days from the issuance of this Order, correct the deficiencies identified in the accompanying Memorandum Opinion; or,

---

<sup>1</sup> See Docket No. 702(i)-08-01, Sept. 4, Memorandum Opinion at 17-18 n.14.

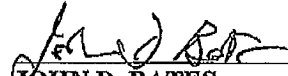
~~TOP SECRET//COMINT//ORCON,NOFORN~~



~~TOP SECRET//COMINT//ORCON,NOFORN~~



(b) cease the implementation of the Certifications insofar as they permit the acquisition of MCTs as to which the "active user" is not known to be a tasked selector.

ENTERED this 3rd day of October, 2011, at 4:55 p.m. Eastern Time.



**JOHN D. BATES**  
Judge, United States Foreign  
Intelligence Surveillance Court

~~TOP SECRET//COMINT//ORCON,NOFORN~~

I,  Deputy Clerk,  
FISC, certify that this document  
is a true and correct copy of  
the original 

(b)(6)

# Exhibit 21

IN UNITED STATES DISTRICT COURT  
FOR THE DISTRICT OF COLUMBIA

LARRY KLAYMAN, *et. al*

Plaintiffs,

v.

BARACK HUSSEIN OBAMA II, *et. al*

Defendants.

Civil Action Nos. 13-cv- 851  
13-cv-881

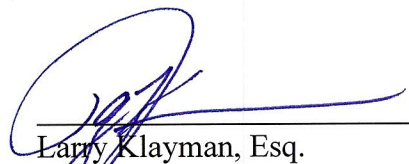
**NOTICE TO APPEAR AT ORAL ARGUMENTS**

TO DEFENDANT NATIONAL SECURITY AGENCY AND ITS ATTORNEY OF RECORD:

**NOTICE IS HEREBY GIVEN** that the records custodian or another qualified employee of the Defendant National Security Agency is hereby required to appear at the oral arguments scheduled to take place on November 18, 2013 at 11:30 a.m., in the U.S. District Court for the District of Columbia, Courtroom 18, located at 333 Constitution Ave, NW, Washington, D.C. 20001 to authenticate the documents set forth in the attached *Touhy* letter to the NSA of November 13, 2013.

Dated: November 13, 2013

Respectfully submitted,



Larry Klayman, Esq.  
Attorney at Law  
D.C. Bar No. 334581  
2020 Pennsylvania Ave. NW, Suite 800  
Washington, DC 20006

Tel: (310) 595-0800

CERTIFICATE OF SERVICE

I HEREBY CERTIFY that on this 13th day of November, 2013 a true and correct copy of the foregoing Notice to Appear for Oral Argument (Civil Action Nos. 13-cv- 851 and 13-cv-881) was served via U.S. Mail and E-mail upon the following:

James R. Whitman  
U.S. DEPARTMENT OF JUSTICE  
P.O. Box 7146  
Washington, DC 20044  
(202) 616-4169  
Fax: 202-616-4314  
Email: james.whitman@usdoj.gov

James J. Gilligan  
Special Litigation Counsel  
Civil Division, Federal Programs Branch  
U.S. Department of Justice  
P.O. Box 883  
Washington, D.C. 20044  
(202) 514-3358  
Email: James.Gilligan@usdoj.gov

Attorneys for Defendants.

Respectfully submitted,



Larry Klayman, Esq.  
D.C. Bar No. 334581  
Klayman Law Firm  
2020 Pennsylvania Ave. NW, Suite 345  
Washington, DC 20006  
Tel: (310) 595-0800



November 13, 2013

**URGENT**

Via U.S. Mail and Email

**TOUHY REQUEST FOR DOCUMENTS AND EMPLOYEE TESTIMONY**

Office Of General Counsel  
National Security Agency  
9800 Savage Road  
Ft. George G. Meade, MD 20755

James J. Gilligan, Esq.  
U.S. DEPARTMENT OF JUSTICE  
CIVIL DIVISION, FEDERAL PROGRAMS BRANCH  
20 Massachusetts Avenue, NW  
Room 5138  
Washington, DC 20001

Re: Klayman v. Obama, et al. (Nos. 13-cv-851, 13-cv-881, D.C. District Court) -- Hearing of November 18, 2013, at 11:30 a.m.

Ladies and Gentlemen:

Pursuant to the request of the undersigned, Larry Klayman, this letter serves as a "Touhy Request," requesting the documents and testimony of a National Security Agency employee. *See Touhy v. Ragen*, 340 U.S. 462 (1951). This request is being sent with the enclosed notice to appear at a hearing that is being sent with regard to the above styled case. A hearing is being held on Monday, November 18, 2013, at 11:30 a.m. in Courtroom 18 of the U.S. District Court for the District of Columbia, located at 333 Constitution Ave, NW, Washington, D.C. 20001. A notice to appear is attached and enclosed.

Background.

On April 25, 2013, the Honorable Roger Vinson, a judge of the U.S. Foreign Intelligence Surveillance Court ("FISC"), issued a top-secret order compelling the disclosure of all call detail records in possession of Verizon Telecommunication for analysis by the National Security Agency ("NSA") on an ***ongoing daily basis***.<sup>1</sup> On June 5, 2013, based on the disclosures of whistleblower, Edward Snowden, who fled the United States for fear of government reprisal, *The*

<sup>1</sup> *See, In re Application of the FBI for an Order Requiring the Production of Tangible Things from Verizon Bus. Network Servs., Inc. on Behalf of MCI Commc'n Servs., Inc. d/b/a Verizon Bus. Servs.*, No. BR 13-80 (FISA Ct. Apr. 25, 2013) ("Verizon Order").

*Guardian* publicly revealed this previously classified order in an article entitled “NSA collecting phone records of millions of Verizon customers daily. Exclusive: Top secret order requiring Verizon to hand over all call data shows scale of domestic surveillance under Obama.”<sup>2</sup>

Prior to this disclosure, the American people had no reasonable opportunity to discover the existence of this surveillance program or its clear violation of statutory and constitutional protections.

Based on the disclosures of whistleblower Edward Snowden in *The Guardian*, the Verizon Order showed, for the first time, that the communication records of U.S. citizens are being collected indiscriminately and in bulk—regardless of whether there is reasonable suspicion or any “probable cause” of any wrongdoing.

On June 9, 2013, the undersigned filed suit challenging the legality of the government's secret and illicit government scheme to systematically gather, intercept and analyze vast quantities of domestic telephonic communications and “metadata” wholly within the United States by implementing a highly classified, unlawful mass call tracking surveillance program run by the NSA. The federal government and the NSA have far exceeded their statutory authority and, as such, violated the First, Fourth, and Fifth Amendments of the U.S. Constitution in addition to Section 215 of the Patriot Act, which is the basis of the subject lawsuit.

The information requested below is required by the undersigned and the other plaintiffs in order to determine the full scope of the Constitutional violations that have been occurring as a result of the NSA's illegal data collection programs.

Requested Testimony.

- 1) A custodian of records is required to authenticate internal memorandum and other such correspondence between the NSA and outside agencies, members of Congress, and any other documents in possession of the plaintiffs, including but not limited to the following:
  - a) United States Government Memorandum of 3 May 2012 (OC-034-12)
  - b) Memorandum for Staff Director, House Permanent Select Committee on Intelligence of 25 February 2009 (GC/009/09)
  - c) FAA Certification Renewals With Caveats on 2011-10-12 0850
  - d) Correspondence of NSA director Keith B. Alexander to Senators Ron Wyden and Mark Udall on 25 June 2013
  - e) Correspondence of Senator Chuck Grassley to Dr. George Ellard, Inspector General of the National Security Agency of August 27, 2013

---

<sup>2</sup> In the days after *The Guardian* disclosed the Verizon Order, the Director of National Intelligence, James Clapper, acknowledged its authenticity and issued a statement indicating that the FISC had renewed it. See Office of the Dir. Of Nat'l Intelligence, *DNI Statement on Recent Unauthorized Disclosure of Classified Information* (June 6, 2013), <http://1.usa.gov/13jwuFc>. See also, Office of the Dir. Of Nat'l Intelligence, *Foreign Intelligence Surveillance Court Renews Authority to Collect Telephony Metadata* (July 19, 2013), <http://1.usa.gov/12ThY1T>.

- f) Correspondence of Dr. George Ellard, Inspector General of the National Security Agency to Senator Chuck Grassley on 11 September 2013
- g) Powerpoint slides of PRISM/US-984XN Overview

These documents are attached to and enclosed with this letter.

- 2) Testimony by a person or persons within the NSA who are familiar with the telephony and metadata collection performed by the NSA on the American people, including but not limited to data collected by a collaboration with Verizon Communications and all other telephone and/or internet companies such as Skype, Google, Youtube, AOL, YAHOO!, Facebook, Paltalk, AT&T, Sprint, and Microsoft.

This Testimony is Not Available From Another Source.

This testimony and the subject documents are only in the possession of the NSA and only the NSA will be able to authenticate the documents obtained by the undersigned. In addition, only the NSA knows the nature and full extent of the surveillance that is being performed and will be the only ones capable of testifying about it.

Production is Appropriate in Light of Any Relevant Privilege.

There are no relevant privileges. The NSA has been secretly, and in violation of the Patriot Act and the U.S. Constitution, been performing surveillance on the American people without any probable cause or reasonable suspicion. Neither the government nor the NSA can present any relevant privilege that will allow them to act in clear violation of the law.

Production Is Appropriate Under The Applicable Rules Of Discovery Or The Procedures Governing The Case Or Matter In Which The Demand Arose.

The Federal Rules of Civil Procedure and Evidence apply since the presiding jurisdiction is the U.S. District Court for the District of Columbia. Under the Federal Rules of Evidence, Rule 401, evidence is relevant if: (a) it has any tendency to make a fact more or less probable than it would be without the evidence; and (b) the fact is of consequence in determining the action.

Any evidence of the extent of the NSA's surveillance is directly relevant to the claims and allegations made by the undersigned and the other plaintiffs in the above styled lawsuit. The method and amount of data collected by the NSA is of direct consequence to whether they are acting in violation the Patriot Act and the U.S. Constitution.

Disclosure Would Not Violate Any Statutes, Responsibilities, Regulations, or Directives of the NSA, Nor Would it Reveal Classified Information.

The undersigned seeks to verify the authenticity of information that has already been release to the American people. The disclosure of such information has already been made, and the authentication is only required for the legal proceedings.



Description of Testimony Sought.

As described above, the undersigned seeks the testimony of a custodian of records who can authenticate the documents currently in his possession. In addition, the undersigned is requesting an employee or employees who can describe the method and amount of telephony and metadata that is collected by the NSA.

Yours truly,

A handwritten signature in blue ink, appearing to be 'L. Klayman', with a long horizontal line extending to the right.

Larry Klayman

UNITED STATES GOVERNMENT  
Memorandum

OC-034-12

DATE: 3 May 2012

REPLY TO  
ATTN OF: SID Oversight & Compliance

SUBJECT: (U//FOUO) NSAW SID Intelligence Oversight (IO) Quarterly Report – First Quarter Calendar Year 2012 (1 January – 31 March 2012) – EXECUTIVE SUMMARY

TO: SIGINT Director

---

**I. (U) Overview**

(U//FOUO) The attached NSAW SID Intelligence Oversight (IO) Quarterly Report for the First Quarter Calendar Year 2012 (1 January – 31 March 2012) identifies NSAW SID compliance with E.O. 12333, DoD Regulation 5240.1-R, NSA/CSS Policy 1-23, USSID SP0018, and all related policies and regulations.

(U//FOUO) Detailed incident narratives are provided in the attached annexes. The number of incidents in each category and a reference to the annex related to each incident category are contained in the body of the report.

(U//FOUO) As part of SID Oversight and Compliance's (SV) charge to provide comprehensive trends and analysis information as it pertains to incidents of non-compliance, this Executive Summary provides analysis and evaluation of incidents reported throughout the current quarter to better address the "whys" and "hows" behind NSAW SID's compliance posture.

(U//FOUO) Section II, Metrics, has been broken down into several sub-sections: metrics and analysis of NSAW SID-reported incidents by authority, type, root cause, and organization. Also included is an assessment of how incidents were discovered (i.e., methods of discovery) for SID-reported incidents (see **Figure 7**).

(U//FOUO) Significant Incidents of Non-compliance and Report Content follow in Sections III and IV, respectively.

(S//REL) Overall, the number of incidents reported during 1QCY12 increased by 11% as compared to the number of incidents reported during 4QCY11. This included a rise in the number of E.O. 12333 incidents, as well as for incidents across all FISA authorities. The majority of incidents in all authorities were database query incidents due to human error. Of note, S2 continued to be the NSAW SID organization with the largest number of reported incidents (89%), although S2 experienced an overall decrease in reported incidents. SV noted an overall improvement in timeliness regarding 1QCY12 IO Quarterly Report submissions from the SID elements.

**II. (U) Metrics**

**a. (U//FOUO) NSA SID-reported Incidents by Authority**

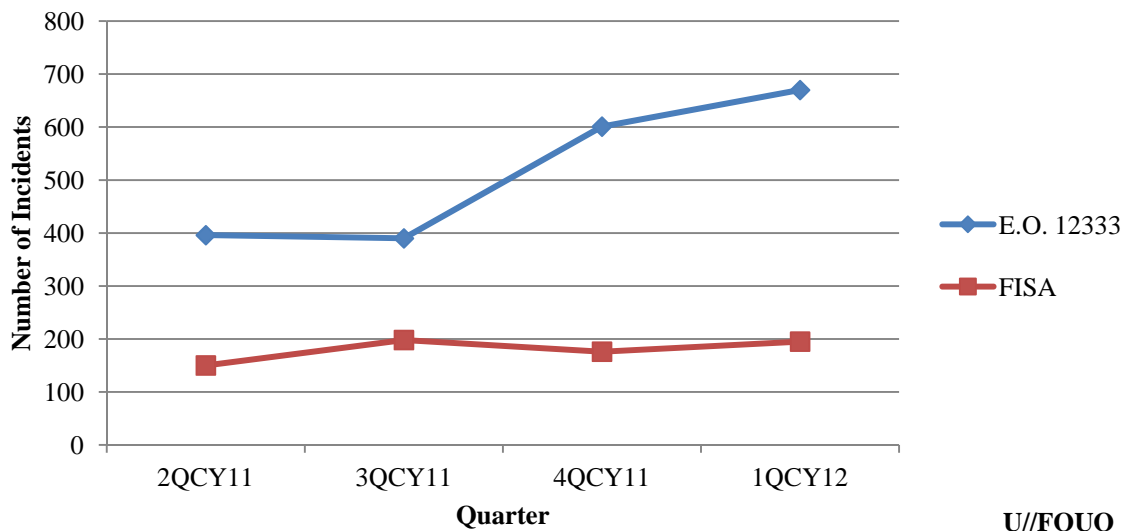
(TS//SI//REL TO USA, FVEY) **Figures 1a-b** compares all categories of NSA SID-reported incidents (collection, dissemination, unauthorized access, and retention) by Authority for 2QCY11 – 1QCY12. From 4QCY11 to 1QCY12, there was an overall increase in incidents of 11%. There was also an increase of 11% for both E.O. 12333 and FISA incidents. The increase in incidents reported for 1QCY12 was due to an increase in the number of reported Global System for Mobile Communications (GSM) roamer<sup>1</sup> incidents, which may be attributed to an increase in Chinese travel to visit friends and family for the Chinese Lunar New Year holiday.

(U//FOUO) **Figure 1a:** Table of the Number of NSA SID-reported Incidents by Authority  
(U//FOUO)

	2QCY11	3QCY11	4QCY11	1QCY12
<b>E.O. 12333</b>	396	390	601	670
<b>FISA</b>	150	198	176	195
<b>TOTAL</b>	<b>546</b>	<b>588</b>	<b>777</b>	<b>865</b>

(U//FOUO)

(U//FOUO) **Figure 1b:** Line Graph of the Number of NSA SID-reported Incidents by Authority  
U//FOUO



(U//FOUO)

(TS//SI//NF) **FISA Incidents:** As reflected in **Figures 1a-b**, during 1QCY12, NSA SID reported a total of 195 FISA incidents, 185 of which were associated with unintentional collection. NSA SID also reported 6 incidents of unintentional dissemination under FISA authority and 4 incidents of unauthorized access to Raw

<sup>1</sup> (U//FOUO) Roaming incidents occur when a selector associated with a valid foreign target becomes active in the U.S.

SIGINT FISA data. **Figure 2** illustrates the most common root causes for incidents involving FISA authorities as determined by SV.

- 63% (123) of 1QCY12 FISA incidents can be attributed to Operator Error as the root cause, and involved:
  - Resources ( i.e., inaccurate or insufficient research information and/or workload issues (60);
  - Lack of due diligence (i.e., failure to follow standard operating procedures) (39);
  - Human error (21) which encompassed:
    - Broad syntax (i.e., no or insufficient limiters / defeats / parameters) (12);
    - Typographical error (6);
    - Query technique understood but not applied (2); and
    - Incorrect option selected in tool (1); and
  - Training and guidance (i.e., training issues) (3).

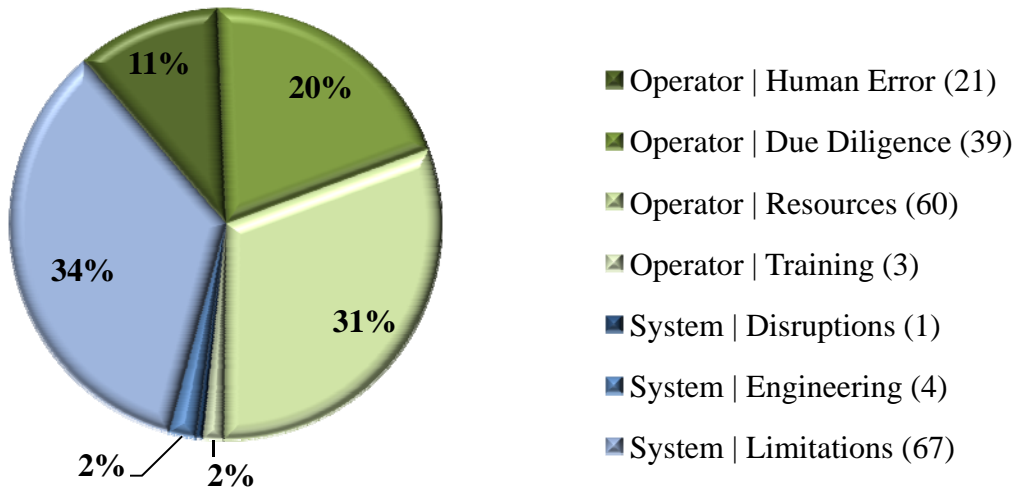
(U//FOUO) The Resources root cause category accounted for the largest percentage of Operator Error incidents under FISA authorities for 1QCY12. Analysis identified that these incidents could be reduced if analysts had more complete and consistent information available about selectors and/or targets at the time of tasking and if analysts consistently applied rules for conducting queries.

- 37% (72) of 1QCY12 FISA incidents can be attributed to System Error as the root cause, and involved:
  - System limitations (i.e., system lacks the capability to ‘push’ real-time travel data out to analysts, system/device unable to detect changes in user) (67);
  - System engineering (i.e., system/database developed without the appropriate oversight measures, data flow issues, etc.) (4); and,
  - System disruptions (i.e., glitches, bugs, etc.) (1).

(U//FOUO) The System Limitations root cause category accounted for the largest percentage of System Error incidents under FISA authorities for 1QCY12. The largest number of incidents in the System Limitations category account for roamers where there was no previous indications of the planned travel. These incidents are largely unpreventable. Consistent discovery through the Visitor Location Register (VLR) occurs every quarter and provides analysts with timely information to place selectors into candidate status or detask. Analysis identified that these incidents could be reduced if analysts removed/detasked selectors more quickly upon learning that the status of the selector had changed and more regularly monitored target activity. This analysis indicates that continued research on ways to exploit new technologies and researching the various aspects of personal communications systems to include GSM, are an important step for NSA analysts to track the travel of valid foreign targets.

(U//FOUO) **Figure 2: 1QCY12 FISA Incidents – Root Causes**

U//FOUO



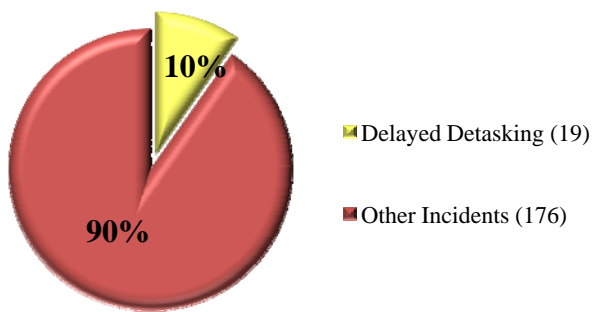
**Total: 195**

U//FOUO

(TS//SI//REL TO USA, FVEY) **Delayed Detasking FISA Incidents:** As reflected in **Figures 1a-b**, during 1QCY12, NSAW SID reported a total of 195 FISA incidents. 19 (10%) of the total FISA incidents were associated with detasking delays. Of the 19 delayed detasking incidents, 12 (63%) of these incidents occurred under NSA FISA Authority, 5 (27%) occurred under FAA 702 Authority, 1(5%) occurred under FAA 704 Authority, and 1 (5%) occurred under FAA 705(b) Authority. **Figure 3a** illustrates the detasking delay incidents versus all other FISA incidents reported during 1QCY12. **Figure 3b** illustrates the detasking delay incidents by FISA Authority reported during 1QCY12.

(U//FOUO) **Figure 3a: 1QCY12 Detasking FISA Incidents vs. All other FISA incidents**

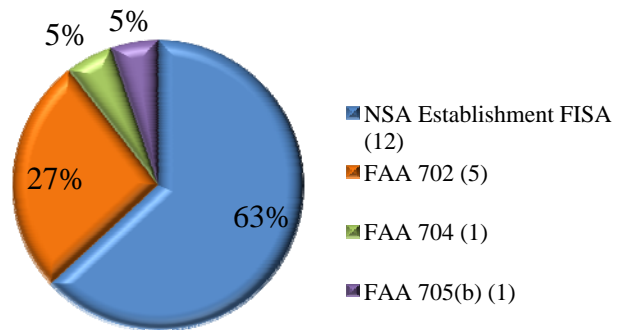
U//FOUO



**Total: 195**

(U//FOUO) **Figure 3b: 1QCY12 FISA Incidents by Authority – Delayed Detaskings**

U//FOUO



**Total: 19**

U//FOUO

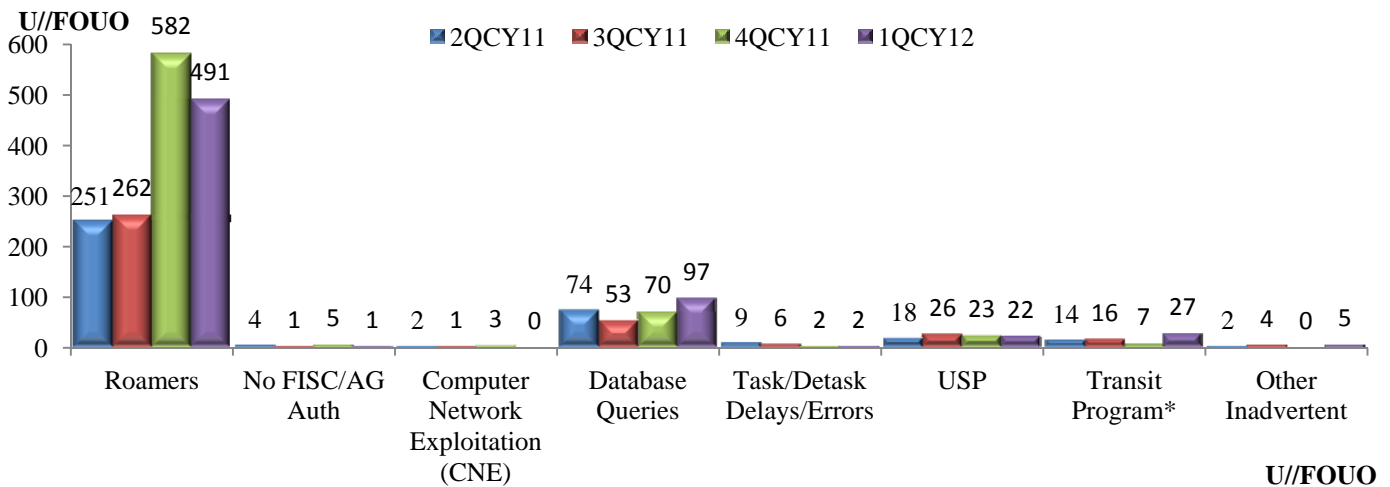
U//FOUO

(TS//SI//REL TO USA, FVEY) As depicted in Figures 3a and 3b, of the 19 delayed detasking FISA incidents, 15 (79%) resulted from a failure to detask all selectors, 2 (11%) resulted from analyst not detasking when required, 1 (5%) resulted from partner agency error, and 1 (5%) resulted from all tasking not terminated (e.g., dual route).

**b. NSA SID-reported Collection Incidents by Sub-Type and Authority**

(U//FOUO) **Figures 4a-b** depicts NSA SID-reported collection incidents by Authority (E.O. 12333 and all FISA Authorities), and identifies the primary sub-types for those incidents. An explanation of the more prominent collection incident sub-types follows the graphs.

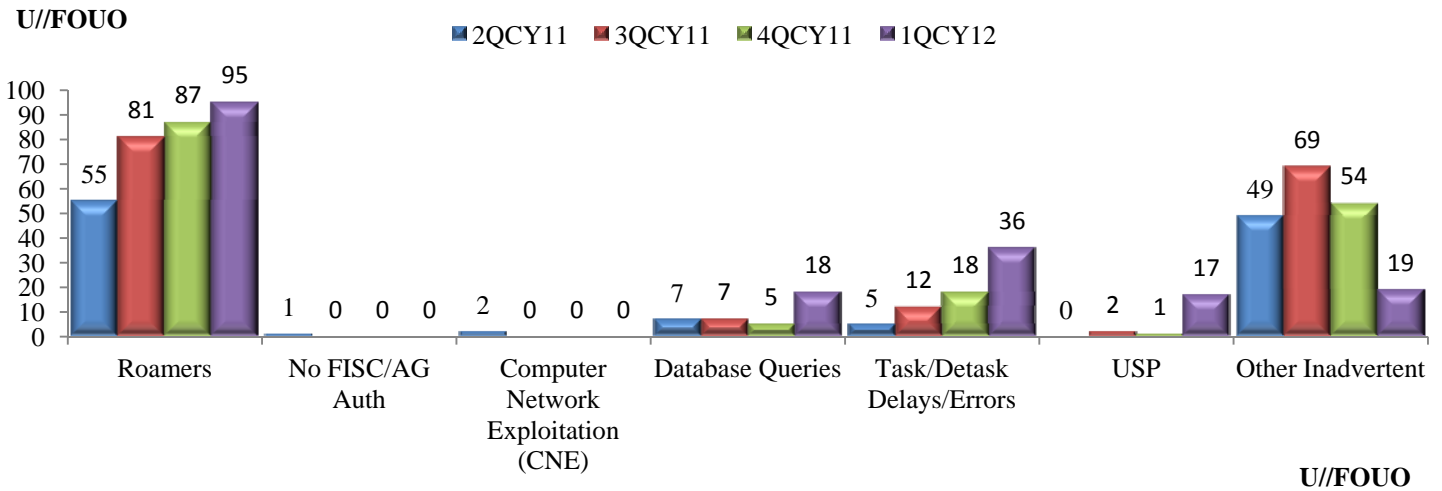
(U//FOUO) **Figure 4a:** NSA SID-reported Collection Incidents Under E.O. 12333 Authority



(U//FOUO) **Figure 4a:** During 1QCY12, NSA SID reported a 39% increase of database query incidents under E.O. 12333 Authority. Human Error accounted for 74% of E.O.12333 database query incidents.

(TS//SI//REL TO USA, FVEY) **International Transit Switch Collection\*:** International Transit switches, FAIRVIEW (US-990), STORMBREW (US-983), ORANGEBLOSSOM (US-3251), and SILVERZEPHYR (US-3273), are Special Source Operations (SSO) programs authorized to collect cable transit traffic passing through U.S. gateways with both ends of the communication being foreign. When collection occurs with one or both communicants inside the U.S., this constitutes inadvertent collection. From 4QCY11 to 1QCY12, there was an increase of transit program incidents submitted from 7 to 27, due to the change in our methodology for reporting and counting of these types of incidents. (\*See Annex G in SID’s 1QCY12 IO Quarterly Report for additional details regarding these incidents.)

(U//FOUO) **Figure 4b: NSAW SID-reported Collection Incidents Under All FISA Authorities**



(U//FOUO) **Figure 4b:** During 1QCY12, NSAW SID reported an increase of 9% of roamer incidents under all FISA Authorities. There was also a 260% increase in database query FISA Authority incidents during 1QCY12. Human Error accounted for the majority of all FISA Authorities database query incidents (74%).

(U//FOUO) **Roamers:** Roaming incidents occur when valid foreign target selector(s) are active in the U.S. Roamer incidents continue to constitute the largest category of collection incidents across E.O. 12333 and FAA authorities. Roamer incidents are largely unpreventable, even with good target awareness and traffic review, since target travel activities are often unannounced and not easily predicted.

(S//SI//NF) **Other Inadvertent Collection:** Other inadvertent collection incidents account for situations where targets were believed to be foreign but who later turn out to be U.S. persons and other incidents that do not fit into the previously identified categories.

(TS//SI//REL TO USA, FVEY) **Database Queries:** During 1QCY12, NSAW SID reported a total of 115 database query incidents across all Authorities, representing a 53% increase from 4QCY11. E.O. 12333 Authority database query incidents accounted for 84% (97) of the total, and all FISA Authorities database query incidents accounted for 16% (18).

(U//FOUO) **Figure 5** illustrates the most common root causes for incidents involving database queries as determined by SV.

- 99% (114) of the 1QCY12 database query incidents are attributed to Operator Error as the root cause, and involved:
  - Human error (85) which encompassed:
    - Broad syntax (i.e., no or insufficient limiters / defeats / parameters) (55);
    - Typographical error (17);
    - Boolean operator error (6);
    - Query technique understood but not applied (4);
    - Not familiar enough with the tool used for query (2); and

- Incorrect option selected in tool (1)
- Lack of due diligence (i.e., failure to follow standard operating procedure) (13)
- Training and guidance (i.e., training issues) (9); and
- Resources (i.e., inaccurate or insufficient research information and/or workload issues) (7).

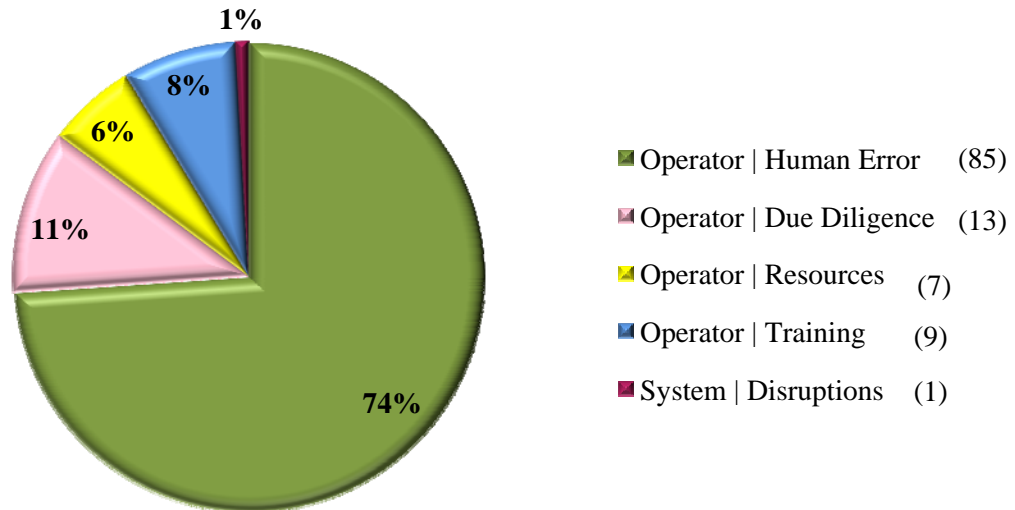
(U//FOUO) The remaining 1 database query incident can be attributed to System Error as the root cause and occurred due to a mechanical error with the tool.

(U//FOUO) Analysis identified that the number of database query incidents could be reduced if analysts more consistently applied rules/standard operating procedures (SOPs) for conducting queries.

(S//SI//NF) Auditors continue to play an important role in the discovery of database query incidents, identifying 70 (61%) of the 115 reported database query incidents.

(U//FOUO) **Figure 5: 1QCY12 Database Query Incidents – Root Causes**

**U//FOUO**



**Total: 115**

**U//FOUO**

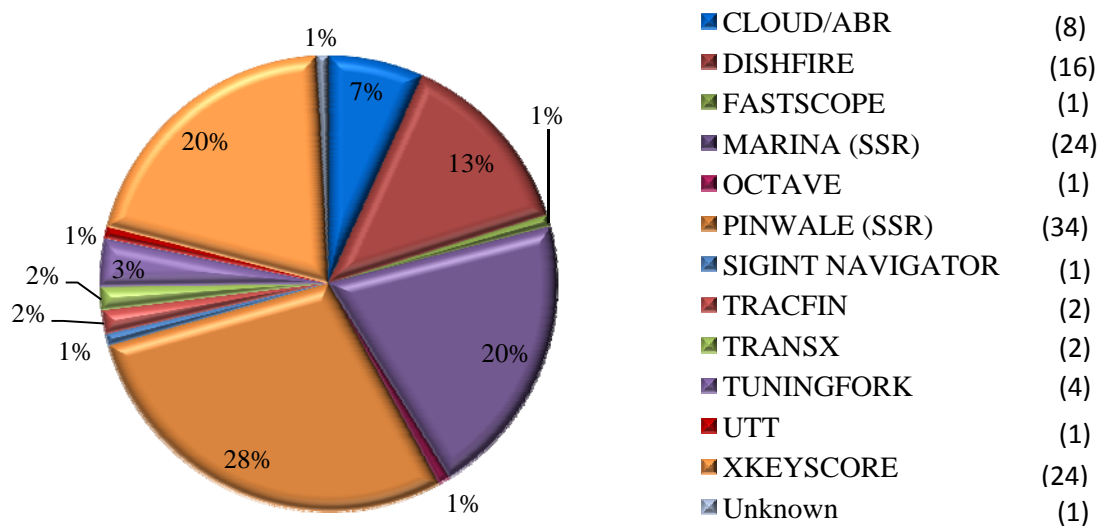
(TS//SI//REL TO USA, FVEY) Of the 115 database query incidents reported for 1QCY12, **Figure 6** identifies the database involved and the associated percentage of the total. Databases considered to be Source Systems of Record (SSR) have been labeled as such.

(TS//SI//REL TO USA, FVEY) Note that the total number of databases involved in the database query incidents in **Figure 6** does not equal the number of database query incidents reflected in Figure 5 or in the 1QCY12 SID IO Quarterly Report because a database query incident may occur in more than one database.



(U//FOUO) **Figure 6: 1QCY11 Database Query Incidents – Database(s) Involved**

U//FOUO



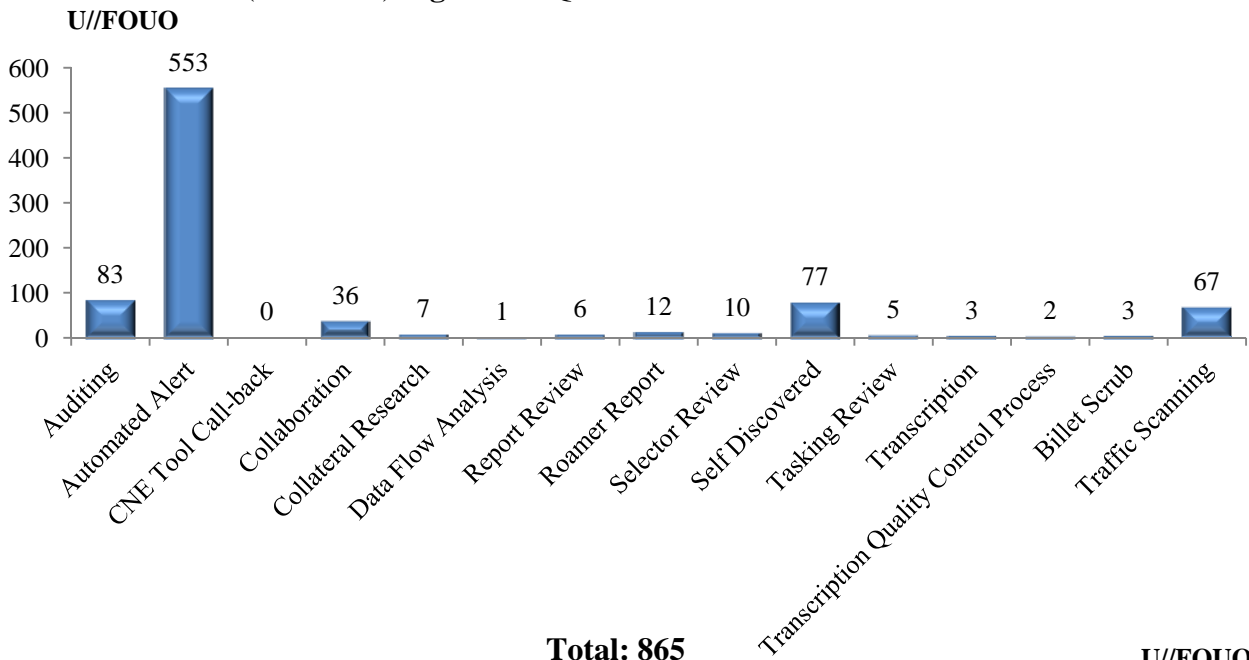
**Total: 119**

U//FOUO

(U//FOUO) **NSAW SID-reported Incidents – Method of Discovery**

(U//FOUO) **Figure 7** depicts the most prominent method(s) of discovery for incidents reported by NSAW SID elements for 1QCY12. As SV’s assessment of root causes matures, and as corrective measures are implemented, identification of how incidents are discovered will provide additional insight into the effectiveness of those methods.

(U//FOUO) **Figure 7: 1QCY12 Incidents – How Discovered**



**Total: 865**

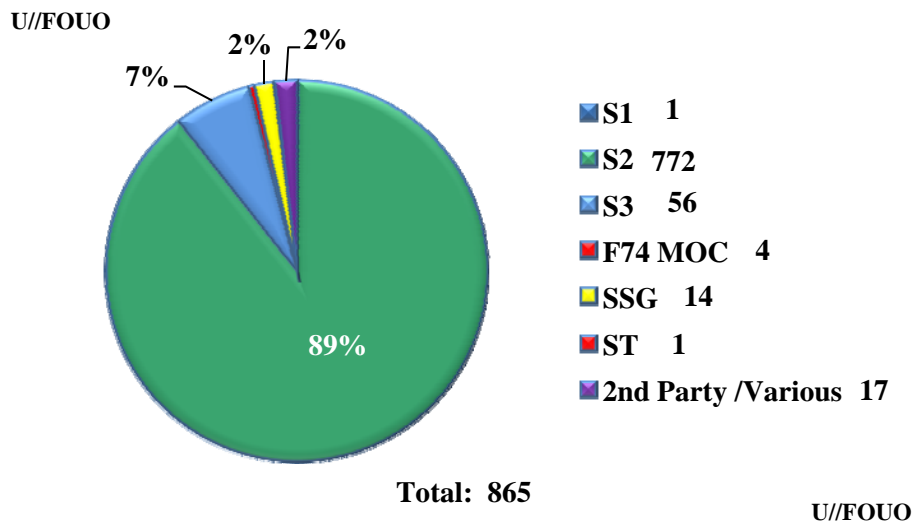
U//FOUO

(U//FOUO) For 1QCY12, of the 865 reported incidents, 553 (64%) were discovered by automated alert. 444, (80%) of the 553 incidents that were discovered by automated alert occurred via the VLR and other analytic tools, such as SPYDER, CHALKFUN, and TransX.

**c. (U//FOUO) NSA SID-reported Incidents by Organization**

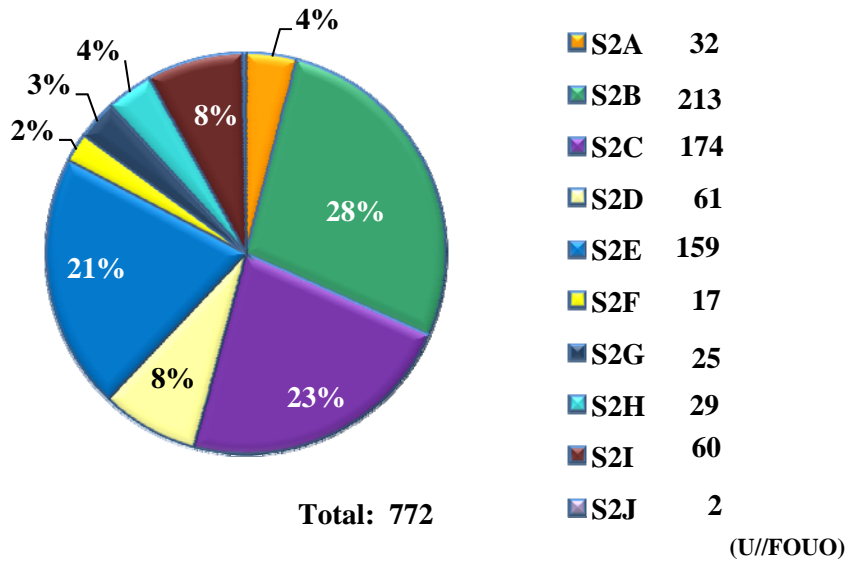
(U//FOUO) **Figure 8** illustrates the total 1QCY12 NSA SID-reported incidents by primary SID Deputy Directorate (DD) level organization. S2, having the largest NSA SID contingent of reported incidents, accounted for 89% of the total incidents for the quarter, a proportion consistent with the overall size of the S2 organization. As compared to 4QCY11, S2 experienced an overall 8% reduction in incidents occurrences.

(U//FOUO) **Figure 8:** 1QCY12 Incidents by NSA SID Organization



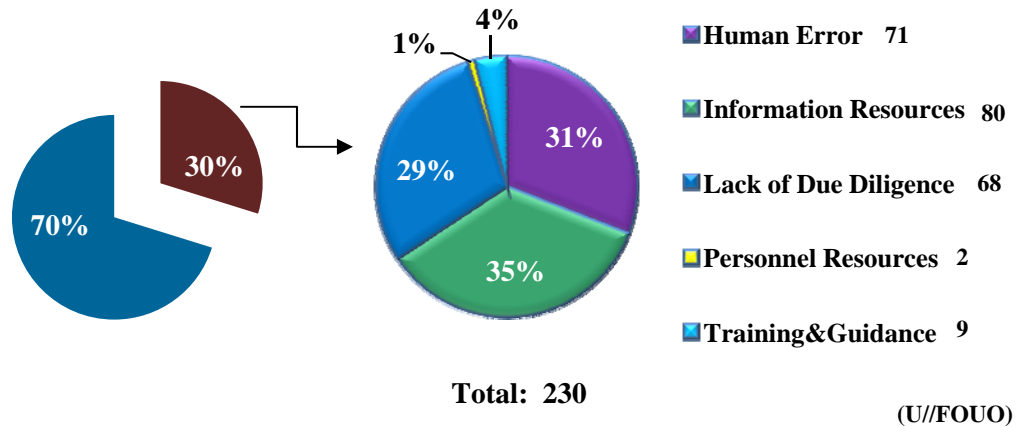
(U//FOUO) **Figure 9** provides a look into S2 (by Product Line) as the NSA SID organization with the largest number of reported incidents. For 1QCY12, three Product Lines accounted for 72% of S2's reported incidents. These Product Lines were: the and Korea Division (S2B) with 28% of the reported incidents, the International Security Issues Division (S2C) with 23% of the reported incidents, and the China, and the Office of Middle East & Africa (S2E) with 21% of the incidents. As compared to 4QCY11, this resulted in an increase of 16% for S2B, a reduction of 35% for S2C, and an increase of 9% for S2E. The number of incidents reported by the remaining seven Product Lines held relatively steady from 4QCY11 to 1QCY12.

(U//FOUO) **Figure 9:** 1QCY12 S2 Incidents by Product Line  
(U//FOUO)



(U//FOUO) **Figures 10a-b** illustrates the operator related (**Figure 10a**) and system related (**Figure 10b**) root causes associated with the 772 incidents reported by S2. 30% of the incidents were due to operator related errors that resulted in an incident. 70% of the incidents were due to system related issues that resulted in an incident.

(U//FOUO) **Figure 10a:** 1QCY12 S2 Incidents – Operator Related Root Causes  
(U//FOUO)



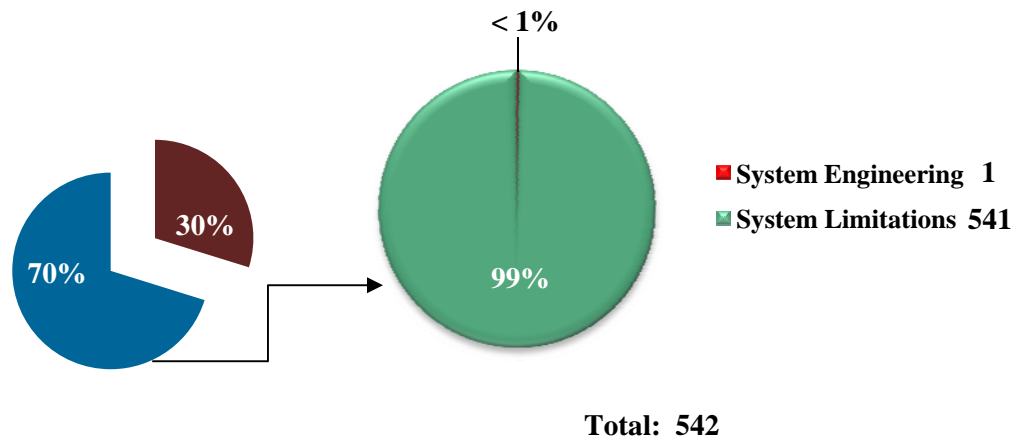
(U//FOUO) 30% of the S2-reported incidents during 1QCY12 are attributed to Operator Error as the root cause, and involved:

- Resources (i.e., inaccurate or insufficient research information and/or workload issues, and personnel resource issues) (82);

- Human error (i.e., selector mistypes, incorrect realm, or improper query) (71);
- Lack of due diligence (i.e., failure to follow standard operating procedures) (68); and
- Training and guidance (i.e., training issues) (9).

(U//FOUO) Analysis found that analysts could reduce the number of incidents if there was more comprehensive research information available at the time of tasking as well as through better use of defeats, more careful review of data entry to avoid typographical errors and omissions, and by following SOPs more consistently.

(U//FOUO) **Figure 10b:** 1QCY12 S2 Incidents – System Related Root Causes  
(U//FOUO)



(U//FOUO)

(U//FOUO) 70% of the S2-reported incidents during 1QCY12 are attributed to system issues as the root cause, and involved:

- System limitations (i.e., system lacks the capability to ‘push’ real-time travel data out to analysts, system/device unable to detect changes in user) (541); and
- System engineering (i.e., data tagging, configuration, design flaws, etc.) (1).

(TS//SI//REL TO USA, FVEY) System Limitations, the largest percentage of System Error root cause, can be attributed to situations where a valid foreign target is found roaming in the United States without indication in raw traffic.

---

### III. (U) Significant Incidents of Non-compliance

(TS//SI//NF) **Business Record (BR) FISA.** As of 16 February 2012, NSA determined that approximately 3,032 files containing call detail records potentially collected pursuant to prior BR Orders were retained on a server and been collected more than five years ago in violation of the 5-year retention period established for BR collection. Specifically, these files were retained on a server used by technical personnel working with the Business Records metadata to maintain documentation of provider feed data formats and performed background analysis to document why certain chaining rules were created. In addition to the BR

work, this server also contains information related to the STELLARWIND program and files which do not appear to be related to either of these programs. NSA bases its determination that these files may be in violation of docket number BR 11-191 because of the type of information contained in the files (i.e., call detail records), the access to the server by technical personnel who worked with the BR metadata, and the listed "creation date" for the files. It is possible that these files contain STELLARWIND data, despite the creation date. The STELLARWIND data could have been copied to this server, and that process could have changed the creation date to a timeframe that appears to indicate that they may contain BR metadata. Additional details regarding this incident can be found in the "Bulk Metadata FISA" Annex, ANNEX R (Item R1) in SID's 1QCY12 IO Quarterly Report.

(S//SI//REL TO USA, FVEY) **Detasking Delay.** Four selectors [REDACTED] remained active after multiple indications were received that the target held a U.S. green card. On 09 March 2012, a South Asia Language Analysis Branch (S2A51) senior linguist was preparing [REDACTED] Division) selectors for OCTAVE migration when it was discovered that the tasking record for [REDACTED] showed that there were four selectors that were in active status even though his tasking file indicated he held a U.S. green card as of 03 October 2011. On 09 March 2012, the S2A51 senior linguist detasked the four selectors, and on 13 March 2012, the S2A51 senior linguist requested the 881 cuts in NUCLEON based on collection from those four selectors be purged. On 13 March 2012, a senior reporter in the [REDACTED] Reporting Branch (S2A52) researched S2A52's locally held file of [REDACTED] who hold U.S. person status and learned that an S2A52 analyst had indications in intercept on 09 September 2011 [REDACTED] might have a U.S. green card. It was also recorded in the same S2A52 file that S2A52 had submitted a request to the Department of Homeland Security (DHS) [REDACTED] (N.B., the date of the S2A52 request to DHS was not recorded) and learned from DHS on 28 September 2011 that Qureshi had obtained a U.S. green card as of [REDACTED] 2010. The S2A52 senior reporter then checked ANCHORY and discovered that S2A52 had issued 32 reports between [REDACTED] 2010 and [REDACTED] 2011. On 14 March 2012, S2A5 submitted a request for Retroactive Dissemination Authority for the 32 reports which contained the name of [REDACTED]. The Customer Relationships, Information Sharing Services Branch (S12) approved ISS/BDA-068-12 on 16 March 2012. Serialized dissemination of U.S. person information did occur. On 13 March 2012, the S2A51 senior linguist who found that these numbers [REDACTED] had not been detasked reminded the other two members of the Governmental Unified Targeting Tool (UTT) Group for S2A5 to check all S2A5 databases for officials who have U.S. (and Second Party person) status before submitting selectors for tasking. Additional details regarding this incident can be found in the Unintentional Collection under E.O. 12333 Authority Annex, "Collection as a Result of Tasking Errors or Detasking Delays", ANNEX E (Item E1) and in the "Unintentional Dissemination of U.S. Person Information Collected Under E.O. 12333, FISA, and FAA Authorities", Annex M (Item M15) in SID's 1QCY12 IO Quarterly Report.

(C//REL TO USA, FVEY) **Unauthorized Access.** On 29 December 2011, a Cryptanalysis and Exploitation (CES)/Office of Target Pursuit (S31174) Branch Chief discovered that CES personnel had likely been inappropriately granted access to NSA Establishment FISA data. Multiple external factors contributed to this situation. First, in 2002, RAGTIME was changed to encompass both NSA Establishment FISA and FBI FISA, but due to insufficient notice regarding this modification, CES continued to apply the earlier rule that RAGTIME applied only to NSA Establishment FISA data. Second, CES relied on the RAGTIME label in CASPORT for granting access to NSA Establishment FISA data but discovered that CASPORT does not accurately reflect NSA Establishment FISA briefing status. Third, CASPORT often lists NSA-FISA in the

“Oversight” section even though this has nothing to do with a particular user’s access. CES has alerted its workforce to look in the CASPORT “Briefing” section for the NSA Establishment FISA entry and CES-controlled software is being updated regarding data access control. Additional details regarding this incident can be found in the “Unauthorized Access to Raw SIGINT” Annex, ANNEX P (Item P2) in SID’s 1QCY12 IO Quarterly Report.

---


**(U) Report Content**

- **Upcoming Initiatives**

(U//FOUO) During CY12, SV plans to develop ‘score cards’ to capture and illustrate an organization’s reported quarterly activities. SV plans to use this information during scheduled feedback sessions with SID reporting organizations to provide a detailed view into specific areas of high interest or concern arising from analyzing IO Quarterly Report metrics.

- **NSAW SID 1QCY12 IOQ Report Challenges:**

(U//FOUO) SV noted an overall improvement in timeliness regarding 1QCY12 IO Quarterly Report submissions from the SID elements. SV received late submissions from SIGDEV Strategy & Governance (SSG) and SID/Deputy Directorate for Data Acquisition (S3), delaying SV’s preparation of the NSAW SID IO Quarterly Report. SV will continue to focus on outreach with SSG and S3 in order to ensure more complete and timely report submissions.

  
Chief, SID Oversight & Compliance

All redacted  
information exempt  
under (b)(1) and (b)(3)  
except as otherwise  
noted.



~~TOP SECRET//COMINT//NOFORN~~  
NATIONAL SECURITY AGENCY

FORT GEORGE G. MEADE, MARYLAND 20755-6000

Serial: GC/009/09

25 February 2009

MEMORANDUM FOR STAFF DIRECTOR, HOUSE PERMANENT SELECT  
COMMITTEE ON INTELLIGENCE

SUBJECT: (U) Congressional Notification - Incidents of Noncompliance -  
INFORMATION MEMORANDUM

(U) The purpose of this correspondence is to notify the Committee of compliance matters that are currently under review by the Foreign Intelligence Surveillance Court and which relate to subjects of prior testimony to the Congress.

~~(TS//SI//NF)~~ Under two separate sets of orders issued by the Court pursuant to Sections 1841 and 1861 of the Foreign Intelligence Surveillance Act of 1978, as amended ("FISA"), the National Security Agency ("NSA" or "Agency") receives telephony and electronic communications metadata in order to produce foreign intelligence related to the activities of [REDACTED] the [REDACTED]

On 15 January 2009, the Department of Justice ("DoJ") notified the Court that an automated alert process NSA used to compare the telephony metadata against a list of telephone identifiers that were of foreign intelligence interest to NSA's counterterrorism personnel did not operate in conformity with the Court's orders. The Government also advised the Court that NSA had incorrectly described the alert process in prior reports to the Court. As part of a comprehensive review ordered by the Director of NSA, the Agency identified another automated process used to query the telephony metadata that also did not operate in conformity with the Court's orders. The review also identified some manually entered queries that were noncompliant with the Court's orders. None of the compliance incidents resulted in the dissemination of any reporting from NSA to any other department or agency. Upon discovery of these compliance incidents, NSA immediately made changes to its processes to ensure that the Agency is handling and querying the telephony metadata in accordance with the Court's orders. The corrective measures include implementation of controls that prevent any automated process from querying the telephony metadata NSA receives pursuant to the Court's orders and which also guard against manual querying errors.

Derived From: NSA/CSSM 1-52

Dated: 20070108

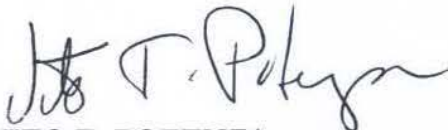
Declassify On: ~~20320108~~

~~TOP SECRET//COMINT//NOFORN~~

~~(TS//SI//NF)~~ In response to the Government's compliance notice, on 28 January 2009, the Court directed the Government to file a brief and supporting documentation describing how the compliance and misreporting incidents occurred so the Court can determine what remedial action, if any, is warranted. Since the Court was aware that there are similarities between NSA's processing of telephony metadata and electronic communications metadata under separate orders, the Court also directed the Government to determine whether NSA has been processing the electronic communications metadata in accordance with the terms of the Court's orders for this category of material. As part of this review, the Government concluded that NSA was processing the electronic communications metadata in accordance with the terms of the Court's orders, with one exception. The review identified one particular process that the Government concluded was not in conformity with the Court's order. NSA had employed the process in a small number of cases to approve queries against the electronic communications metadata. Although the Agency had previously reported the process to the Court [REDACTED] [REDACTED] this process, too, has been discontinued.

~~(S)~~ NSA and DoJ have already identified a number of steps designed to improve the Agency's ability to comply with the relevant orders and implementation of these changes has begun. Also, in addition to notifying the Court, the Government has notified a number of senior Executive Branch officials about these compliance matters. Officials who have received such notification include the President's Intelligence Oversight Board, the Director of National Intelligence, NSA's Inspector General, and the Under Secretary of Defense for Intelligence. My office is also prepared to brief the Committee on these matters at the Committee's convenience.

(U) Should you have any questions, please contact Jonathan E. Miller, Associate Director of Legislative Affairs, at [REDACTED]



VITO T. POTENZA  
General Counsel

Copy Furnished:  
Minority Staff Director, House Permanent  
Select Committee on Intelligence





(TS//SI//NF) FAA Certification Renewals With Caveats  
By [REDACTED] on 2011-10-12 0850

(TS//SI//NF) The FISA Court signed the 2011 FAA Certifications on 3 Oct 2011 – these are valid until 2 Oct 2012, permitting SSO FAA-authorized accesses to continue operations. However, in the 80-page opinion, the judge ordered certain “upstream” or “passive” FAA DNI collection to cease after 30 days, unless NSA implements solutions to correct all deficiencies identified in the opinion document. PRISM operations are not affected by these caveats. All PRISM providers, except Yahoo and Google, were successfully transitioned to the new Certifications. We expect Yahoo and Google to complete transitioning by Friday 6 Oct. Regarding the non-PRISM FAA collection programs, the Court cited targeting and minimization procedures related to collection of Multiple Communications Transactions as “deficient on statutory and constitutional grounds.” SSO, Technology Directorate, OGC, and other organizations are coordinating a response, which includes planning to implement a conservative solution in which the higher-risk collection will be sequestered. It is possible that this higher risk collection contains much of the non-duplicative FAA collection resulting in FAA reporting from upstream accesses. This solution is designed to comply with the judge’s order; however, the judge will have to determine if it does. If the solution is installed, SSO will then work with OPIs and OGC to modify the solution over time such that the filtering process will be optimized to permit more valid collection to be processed and forwarded to OPIs. Finally, in parallel with these efforts, the OGC is contemplating filing an appeal to the ruling.



NATIONAL SECURITY AGENCY  
CENTRAL SECURITY SERVICE  
FORT GEORGE G. MEADE, MARYLAND 20755 8000

25 June 2013

The Honorable Ron Wyden  
United States Senate  
221 Dirksen Senate Office Building  
Washington, DC 20510

The Honorable Mark Udall  
United States Senate  
328 Hart Senate Office Building  
Washington, DC 20510


Dear Senators Wyden and Udall:

Thank you for your letter dated 24 June 2013. After reviewing your letter, I agree that the fact sheet that the National Security Agency posted on its website on 18 June 2013 could have more precisely described the requirements for collection under Section 702 of the FISA Amendments Act. This statute allows for "the targeting of persons reasonably believed to be located outside the United States to acquire foreign intelligence information." 50 U.S.C. 1881(a). The statute provides several express limitations, namely that such acquisition:

- (1) may not intentionally target any person known at the time of acquisition to be located in the United States;
- (2) may not intentionally target a person reasonably believed to be located outside the United States if the purpose of such acquisition is to target a particular, known person reasonably believed to be in the United States;
- (3) may not intentionally target a United States person reasonably believed to be located outside the United States;
- (4) may not intentionally acquire any communication as to which the sender and all intended recipients are known at the time of acquisition to be located in the United States; and
- (5) shall be conducted in a manner consistent with the fourth amendment to the Constitution of the United States. 50 U.S.C. 1881(b).

With respect to the second point raised in your 24 June 2013 letter, the fact sheet did not imply nor was it intended to imply "that NSA has the ability to determine how many American communications it has collected under section 702, or that the law does not allow the NSA to deliberately search for the records of particular Americans." As you correctly state, this point has been addressed publicly. I refer you to unclassified correspondence from the Director of National Intelligence dated 26 July 2012 and 24 August 2012.

NSA continues to support the effort led by the Office of the Director of National Intelligence and the Department of Justice to make publicly available as much information as possible about recently disclosed intelligence programs, consistent with the need to protect national security and sensitive sources and methods.



KEITH B. ALEXANDER  
General, U.S. Army  
Director, NSA/Chief, CSS

Copies Furnished:

The Honorable Dianne Feinstein  
Chairman, Select Committee on Intelligence

The Honorable Saxby Chambliss  
Vice Chairman, Select Committee on Intelligence

## Article

### **For Immediate Release**

August 28, 2013

#### **Grassley Presses for Details about Intentional Abuse of NSA Authorities**

WASHINGTON – Senator Chuck Grassley, Ranking Member of the Senate Judiciary Committee, is asking the Inspector General of the National Security Agency (NSA) to provide additional information about the intentional and willful misuse of surveillance authorities by NSA employees. He's also asking for the Inspector General to provide as much unclassified information as possible.

The Senate Judiciary Committee has oversight jurisdiction over the Foreign Intelligence Surveillance Act (FISA) and the intelligence courts that fall under the act's authority.

"The American people are questioning the NSA and the FISA court system. Accountability for those who intentionally abused surveillance authorities and greater transparency can help rebuild that trust and ensure that both national security and the Constitution are protected," Grassley said.

The text of Grassley's letter is below.

August 27, 2013

Dr. George Ellard, Inspector General  
National Security Agency  
Office of the Inspector General  
9800 Savage Road, Suite 6247  
Fort Meade, MD 20755

Dear Dr. Ellard:

I write in response to media reports that your office has documented instances in which NSA personnel intentionally and willfully abused their surveillance authorities.

For each of these instances, I request that you provide the following information:

- (1) The specific details of the conduct committed by the NSA employee;
- (2) The job title and attendant duties and responsibilities of the NSA employee at the time;
- (3) How the conduct was discovered by NSA management and/or your office;
- (4) The law or other legal authority – whether it be a statute, executive order, or regulation – that your office concluded was intentionally and willfully violated;
- (5) The reasons your office concluded that the conduct was intentional and willful;

- (6) The specifics of any internal administrative or disciplinary action that was taken against the employee, including whether the employee was terminated; and
- (7) Whether your office referred any of these instances for criminal prosecution, and if not, why not?

Thank you for your prompt attention to this important request. I would appreciate a response by September 11, 2013. I also request that you respond in an unclassified manner to the extent possible.

Sincerely,

Charles E. Grassley  
Ranking Member

cc: Honorable Patrick Leahy, Chairman

---

© 2008, Senator Grassley

UNCLASSIFIED



NATIONAL SECURITY AGENCY  
CENTRAL SECURITY SERVICE  
OFFICE OF THE INSPECTOR GENERAL



11 September 2013

Sen. Charles E. Grassley  
Ranking Member  
Committee on the Judiciary  
United States Senate  
152 Dirksen Senate Office Building  
Washington, DC 20510

Senator Grassley:

I write in response to your letter of 27 August 2013 requesting information about intentional and willful misuse of surveillance authorities.

Since 1 January 2003, there have been 12 substantiated instances of intentional misuse of the signals intelligence (SIGINT) authorities of the Director of the National Security Agency. The NSA Office of the Inspector General (OIG) currently has two open investigations into alleged misuse of SIGINT and is reviewing one allegation for possible investigation.

**1. Civilian Employee, Foreign Location**

In 2011, before an upcoming reinvestigation polygraph, the subject reported that in 2004, "out of curiosity," he performed a SIGINT query of his home telephone number and the telephone number of his girlfriend, a foreign national. The SIGINT system prevented the query on the home number because it was made on a US person. The subject viewed the metadata returned by the query on his girlfriend's telephone.

The appropriate OIG conducted an investigation. The subject's actions were found to be in violation of United States Signals Intelligence Directive (USSID) 18 (Legal Compliance and U.S. Person Minimization Procedures).

The matter was referred to DoJ in 2011 for possible violations of 18 U.S.C. §641 (embezzlement and theft) and 18 U.S.C. §2511 (interception and disclosure of electronic communications). In 2011, DoJ declined prosecution. The subject retired in 2012 before disciplinary action had been taken.

UNCLASSIFIED

## **2. Civilian Employee, Foreign Location**

In 2005, during a pre-retirement reinvestigation polygraph and interview, the subject reported that, in 2003, he tasked SIGINT collection of the telephone number of his foreign-national girlfriend without an authorized purpose for approximately one month to determine whether she was "involved with any [local] government officials or other activities that might get [him] in trouble."

The NSA OIG determined that the subject's actions violated Executive Order 12333, DoD Regulation 5240.1-R, 5 C.F.R. § 2635.704, and NSA/CSS PMM 30-2, Chapter 366, §§ 1-3 and 3-1.

The OIG's report was shared with the NSA Office of General Counsel (OGC) for an assessment as to whether referral to DoJ was appropriate. Records are insufficient to determine whether a referral was made. The subject retired before the OIG investigation was finalized.

## **3. Civilian Employee, Foreign Location**

In 2004, upon her return from a foreign site, the subject reported to NSA Security that, in 2004, she tasked a foreign telephone number she had discovered in her husband's cellular telephone because she suspected that her husband had been unfaithful. The tasking resulted in voice collection of her husband.

The NSA OIG determined that the subject's actions violated USSID 18, Executive Order 12333, 5 C.F.R. §2635.704, and DoD Regulation 5240.1-R, and possibly 18 U.S.C. §2511 (interception and disclosure of electronic communications).

The OIG report was forwarded to NSA's OGC, which referred the matter to DoJ. The subject of the investigation resigned before the proposed discipline of removal was administered.

## **4. Civilian Employee, Foreign Location**

In 2003, the appropriate OIG was notified that an employee had possibly violated USSID 18. A female foreign national employed by the U.S. government, with whom the subject was having sexual relations, told another government employee that she suspected that the subject was listening to her telephone calls. The other employee reported the incident.

The investigation determined that, from approximately 1998 to 2003, the employee tasked nine telephone numbers of female foreign nationals, without a valid foreign intelligence purpose, and listened to collected phone conversations while assigned to foreign locations. The subject conducted call chaining on one of the numbers and tasked the resultant numbers. He also incidentally collected the communications of a U.S. person on two occasions.

The appropriate agency referred the matter to DoJ. The subject was suspended without pay pending the outcome of the investigation and resigned before discipline had been proposed.

#### **5. Civilian Employee, Foreign Location**

The employee's agency discovered that an employee had misused the SIGINT collection system between 2001 and 2003 by targeting three female foreign nationals.

The appropriate OIG conducted an investigation. The violations were referred to DoJ. The subject resigned before disciplinary action was taken.

#### **6. Civilian Employee, Foreign Location**

As the result of a polygraph examination, it was discovered that an employee had accessed the collection of communications on two foreign nationals.

The employee's agency concluded its investigation in 2006, and the subject received a one-year letter of reprimand (prohibiting promotions, awards, and within-grade increases) and a 10 day suspension without pay. The subject's pending permanent-change-of-station assignment was cancelled, and his promotion recommendation was withdrawn.

#### **7. Civilian Employee, Foreign Location**

In 2011, the NSA OIG was notified that, in 2011, the subject had tasked the telephone number of her foreign-national boyfriend and other foreign nationals and that she reviewed the resultant collection. The subject reported this activity during an investigation into another matter.

The subject asserted that it was her practice to enter foreign national phone numbers she obtained in social settings into the SIGINT system to ensure that she was not talking to "shady characters" and to help mission.

The appropriate OIG found that the subject's actions potentially violated Executive Order 12333, Part 1.7(c)(1), and DoD Regulation 5240.1-R, Procedure 14.

The appropriate OIG referred the matter to DoJ in 2011 as a possible violation of 18 U.S.C. §2511 (interception and disclosure of electronic communications). The subject resigned before disciplinary action had been imposed.

#### **8. Military Member, CONUS Site**

In 2005, the NSA OIG was notified that, on the subject's first day of access to the SIGINT collection system, he queried six e-mail addresses belonging to a former girlfriend, a U.S. person, without authorization. A site review of SIGINT audit discovered the queries four days after they had occurred.



UNCLASSIFIED

The subject testified that he wanted to practice on the system and had decided to use this former girlfriend's e-mail addresses. He also testified that he received no information as a result of his queries and had not read any U.S. person's e-mail.

The NSA OIG concluded that the subject's actions violated USSID 18, Executive Order 12333, 5 CFR §2635.704, and DoD Regulation 5240.1-R.

The OIG report was forwarded to the site command and the OGC. As a result of a Uniform Code of Military Justice Article 15 proceeding, the subject received a reduction in grade, 45 days restriction, 45 days of extra duty, and half pay for two months. It was recommended that the subject not be given a security clearance.

#### **9. Civilian Employee, CONUS Site**

In 2006, the Office of Oversight and Compliance within NSA's Signals Intelligence Directorate informed NSA OIG that, between 2005 and 2006, the subject had without authorization queried in two SIGINT systems the telephone numbers of two foreign nationals, one of whom was his girlfriend. On one occasion, the subject performed a text query of his own name in a SIGINT system.

The OIG investigation found that the subject queried his girlfriend's telephone number on many occasions and her name on two. He testified that he received only one "hit" from the queries on the girlfriend. Another number he queried, that of a foreign national language instructor, returned "insignificant information."

The subject claimed that he queried his name to see if anyone was discussing his travel and the telephone numbers to ensure that there were no security problems.

The OIG concluded that the subject's actions violated Executive Order 12333, 5 C.F.R. §2635.704, DoD Regulation 5240.1-R, and NSA/CSS PMM, Chapter 366 (General Principles for on the job conduct: Use of Government Resources, and Insubordination).

The Agency has been unable to locate records as to whether a referral was made to DoJ. The subject resigned from the Agency before the proposed discipline of removal had been administered.

#### **10. Civilian Employee, CONUS Site**

In 2008, the NSA OIG was notified that a SIGINT audit had discovered a possible violation of USSID 18. An investigation revealed that, while reviewing the communications of a valid intelligence target, the subject determined that the intelligence target had a relative in the U.S. The subject queried the SIGINT system for the e-mail address of the intelligence target in 2008 and used other search terms to obtain information about the target's relative.

UNCLASSIFIED

The OIG concluded that the subject's actions violated USSID 18, Executive Order 12333, and DoD Regulation 5240.1-R.

The OIG report was forwarded to NSA's OGC. The subject received a written reprimand.

**11. Military Member, Foreign Location**

In 2009, the NSA OIG was notified that, in 2009, a military member assigned to a military tactical intelligence unit queried the communications of his wife, who was also a military member stationed in a foreign location. The misuse was discovered by a review of SIGINT audit logs. The investigation by his military unit substantiated the misuse.

Through a Uniform Code of Military Justice Article 15 proceeding, the member received a reduction in rank, 45 days extra duty, and half pay for two months. The member's access to classified information was revoked.

In 2009 this matter was referred to DoJ.

**12. Military Member, Foreign Location**


In 2009, a military unit at a foreign location notified the NSA OIG that, in 2009, a military member had queried a country's telephone numbers to aid in learning that country's language. The misuse was discovered by a review of SIGINT audit logs.

The appropriate branch of the military determined that the analyst's queries were not in support of his official duties and violated USSID 18.

The member's database access and access to classified information were suspended.

I hope that this information satisfies your request.

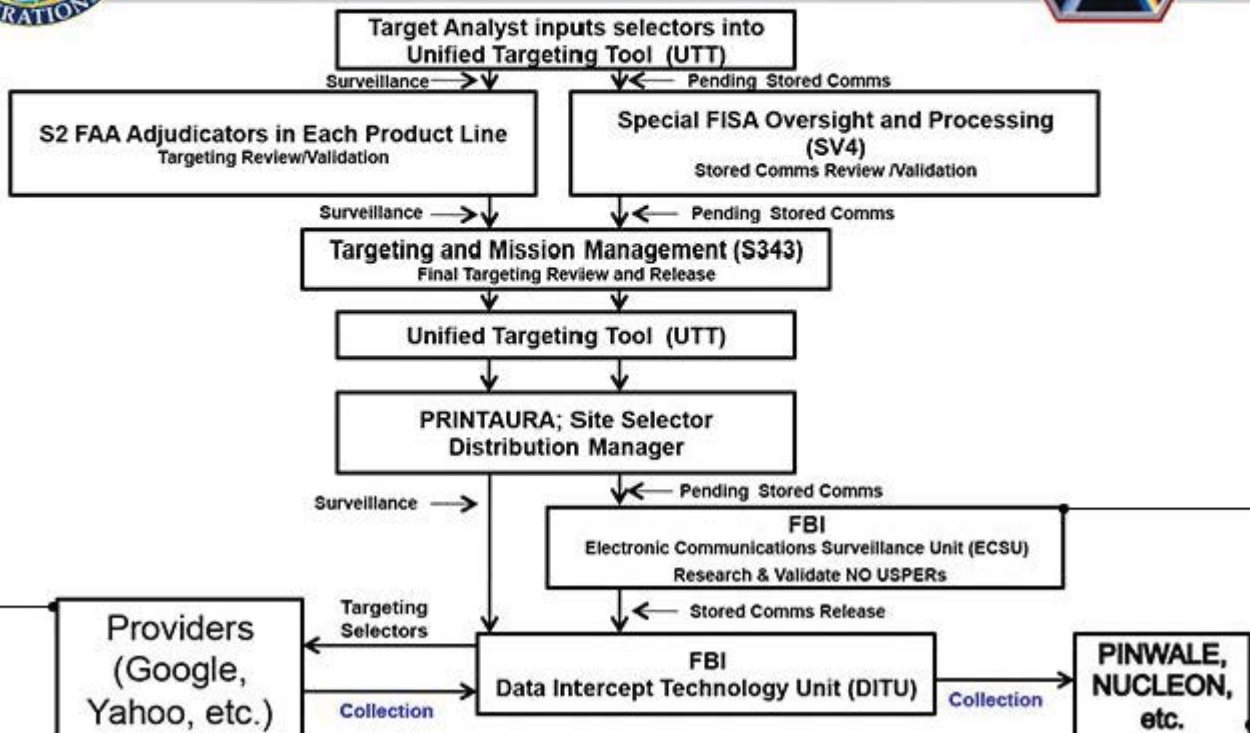
Sincerely,

  
Dr. George Ellard  
Inspector General

cc: Sen. Patrick Leahy



## (TS//SI//NF) PRISM Tasking Process





facebook



Hotmail

YAHOO!

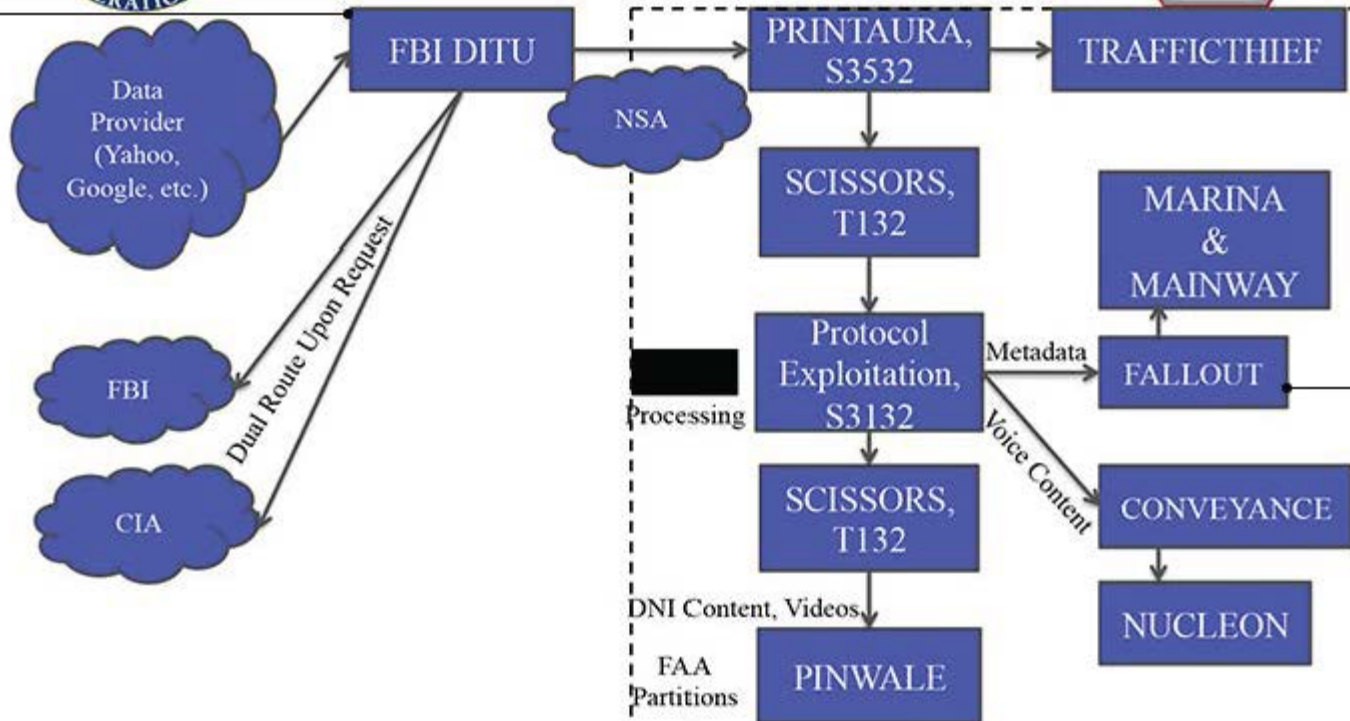


YouTube

AOL mail



## (TS//SI//NF) PRISM Collection Dataflow





facebook



Hotmail



YouTube

AOL mail



## (TS//SI//NF) PRISM Case Notations



P2ESQC120001234

## PRISM Provider

P1: Microsoft  
 P2: Yahoo  
 P3: Google  
 P4: Facebook  
 P5: PalTalk  
 P6: YouTube  
 P7: Skype  
 P8: AOL  
 PA: Apple

Fixed trigraph, denotes  
 PRISM source collection

Year CASN established  
 for selector

Serial #

## Content Type

A: Stored Comms (Search)  
 B: IM (chat)  
 C: RTN-EDC (real-time notification of an e-mail event such as a login or sent message)  
 D: RTN-IM (real-time notification of a chat login or logout event)  
 E: E-Mail  
 F: VoIP  
 G: Full (WebForum)  
 H: OSN Messaging (photos, wallposts, activity, etc.)  
 I: OSN Basic Subscriber Info  
 J: Videos  
 . (dot): Indicates multiple types



facebook



Hotmail



AOL mail



## (TS//SI//NF) REPRISMFISA TIPS

(https:// [REDACTED])



DYNAMIC PAGE - HIGHEST POSSIBLE CLASSIFICATION IS TOP SECRET//SI,TK//ORCON,NOFORN

REPRISMFISA

COUNTERTERRORISM

2013-Apr-05 10:10:28Z

Click on the PRISM icon first  
(from the initial webpage)



## PRISM ENTRIES

Last Lead on Apr 05, 2013 at 12:22 PM GMT

Check the total record status, click on this link

## QUICK LINKS

- See Entry List (Current)
- See Entry List (Expired)
- See Entry List (Current and Expired)
- See NSA List
- See New Records
- Ownership Count

If the total count is much less than this,  
REPRISMFISA is having issues, E-MAIL  
the REPRISMFISA HELP DESK AT

## AND INFORM THEM

Records: 1 - 58 out of 187875 Page: 1 of 254 Records per page: 50

Clear Sort Order Click on column headers to sort. \* columns is not sortable.

## SEARCH

The search form below can be used as a filter to see a partial list of records.

Search For:

AND  OR

Expiration days  
(+ from now)

## Prism Current Entries