

**IN THE UNITED STATES COURT OF APPEALS
FOR THE DISTRICT OF COLUMBIA CIRCUIT**

Larry Klayman, et. al.

Appellees-Cross-Appellants,

v.

Barack Hussein Obama, et al.,

Appellants-Cross-Appellees.

Nos. 14-5004, 14-5016
14-5005, 14-5017

**MOTION FOR LEAVE TO FILE SUPPLEMENTAL BRIEF
IN RESPONSE TO QUESTIONS ASKED AT ORAL ARGUMENT**

Appellees/Cross-Appellants Larry Klayman, Charles Strange, Mary Ann Strange, Matt Garrison, and Michael Ferrari hereby respectfully move this Court for leave to file a Supplemental Brief in response to the questions asked at the oral argument of November 4, 2014.

On November 4, 2014 oral argument was held with regard to the above captioned appeal involving the government's illegal surveillance of Appellees/Cross-Appellants and millions of other similarly situated Americans. During this oral argument, this Court asked Appellees/Cross-Appellants' counsel questions during oral argument which, due to the limited amount of allotted time, did not allow for a full response.

For this reason, Appellees/Cross-Appellants seek to submit the concurrently filed Supplemental Brief which highlights portions of the record and case law which will be helpful to the Court in the determination of this appeal.

Appellees/Cross-Appellants are refiling this supplemental brief as items were unintentionally excluded from the supplemental brief that were originally included in the initial appellate brief.

Appellees/Cross-Appellants have sought consent for this motion from Appellants/Cross-Appellees. Appellants/Cross-Appellees thus far have not responded to Appellees/Cross-Appellants as of the time of this filing.

Appellees/Cross-Appellants will advise the Court of their response.

Dated: November 7, 2014

Respectfully Submitted,

/s/ Larry Klayman

Larry Klayman, Esq.

D.C. Bar No. 334581

2020 Pennsylvania Ave. NW #345

Washington, DC 20006

Tel: (310) 595-0800

Email: leklayman@gmail.com

CERTIFICATE OF SERVICE

I hereby certify that on November 7, 2014, I electronically filed the foregoing Motion for Leave to File a Supplemental Brief in Response to Questions Asked at Oral Argument with the Clerk of the Court for the United States Court of Appeals for the District of Columbia Circuit by using the appellate CM/ECF system. I further certify that I will cause 7 paper copies of this Motion to be filed with the Court.

Respectfully Submitted,

/s/ Larry Klayman

Larry Klayman, Esq.

D.C. Bar No. 334581

2020 Pennsylvania Ave. NW #345

Washington, DC 20006

Tel: (310) 595-0800

Email: leklayman@gmail.com

Nos. 04-5004, 14-5005, 14-5016, 14-5017

IN THE
UNITED STATES COURT OF APPEALS
FOR THE
DISTRICT OF COLUMBIA CIRCUIT

LARRY ELLIOT KLAYMAN ET AL.,
Plaintiffs—Appellees/Cross-Appellants,

— v. —

BARACK HUSSEIN OBAMA ET AL.
Defendants—Appellants/Cross-Appellees.

ON APPEAL FROM THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

**APPELLEES/CROSS-APPELLANTS CORRECTED SUPPLEMENTAL
BRIEF IN RESPONSE TO QUESTIONS ASKED AT ORAL
ARGUMENT**

LARRY KLAYMAN
Attorney at Law
D.C. Bar No. 334581
2020 Pennsylvania Ave. NW, Suite 345
Washington, DC 20006
Phone: (310) 595-0800
Email: leklayman@gmail.com

TABLE OF CONTENTS

TABLE OF AUTHORITIES.....	ii
GLOSSARY.....	iii
INTRODUCTION.....	1
JURISDICTIONAL STATEMENT.....	2
ISSUES PRESENTED FOR REVIEW.....	3
STATEMENT OF THE CASE.....	3
SUMMARY OF THE ARGUMENT.....	3
STANDARD OF REVIEW.....	3
STATUTES AND REGULATIONS.....	4
ARGUMENT.....	4
CONCLUSION.....	20
CERTIFICATE OF COMPLIANCE.....	21
CERTIFICATE OF SERVICE.....	22
EXHIBITS TO SUPPLEMENTAL BRIEF.....	23

TABLE OF AUTHORITIES

Cases

<i>Abram v. Odham</i> , 89 So.2d 334. (1956)	18
* <i>City of Los Angeles v. Lyons</i> , 461 U.S. 95 (1983).....	17
<i>LaDuke v. Nelson</i> , 762 F.2d 1318 (9th Cir. 1985).....	17
<i>Myers v. Hodges</i> , 53 Fla. 197 (1907)	18
* <i>Riley v. California</i> , 134 S.Ct. 2473 (2014).....	22, 23, 24
<i>Smith v. Maryland</i> , 442 U.S. 735 (1979).....	21
<i>Thompson v. North American Stainless, LP</i> , 562 U.S. 170 (2011)	18

Other Authorities

Barton Gellman, <i>NSA broke privacy rules thousands of times per year, audit finds</i> , Washington Post (August 15, 2013), available at http://www.washingtonpost.com/world/national-security/nsa-broke-privacy-rules-thousands-of-times-per-year-audit-finds/2013/08/15/3310e554-05ca-11e3-a07f-49ddc7417125_story.html	8
Jake Gibson, <i>“Too tempting? NSA watchdog details how officials spied on love interests,”</i> FOX News (Sept. 27, 2013), available at http://www.foxnews.com/politics/2013/09/27/too-tempting-nsa-details-how-officials-spied-on-love-interests	8

GLOSSARY

“FISA” refers to the Foreign Intelligence Surveillance Act of 1978

“FISC” refers to the United States *Foreign Intelligence Surveillance Court*

“Section 215” refers to Section 215 of the Patriot Act, Public Law 107–56—Oct. 26, 2001

INTRODUCTION

Appellees/Cross-Appellants hereby incorporate by reference the information required by Rules 28(a) of the Federal Rules of Appellate Procedure and of this Circuit from the brief for Appellees/Cross-Appellants which was filed on August 13, 2014.¹

This supplemental brief is submitted along with a motion for leave to file because this honorable Court asked certain questions of Appellees/Cross-Appellants' counsel during oral argument which, due to the limited amount of time of the oral argument, did not give rise to a full response. Accordingly, this supplemental brief is submitted in order to aid the Court in reaching its ultimate decision, which will have a huge impact on the constitutional rights of not just Appellees/Cross-Appellants but all Americans, to be free from unconstitutional spying on their telephonic communications.

¹ This corrected Supplemental Brief was not changed substantively, but instead was only modified to include a cover page, table of contents, and table of authorities pursuant to Local Rule 28.

JURISDICTIONAL STATEMENT

Plaintiffs invoked the District Court's jurisdiction under 28 U.S.C. § 1331. *See* Appendix ("App.") 39, 74. On December 16, 2013, the District Court entered an order granting in part Plaintiffs' Motion for Preliminary Injunction in *Klayman I* and denying in part Plaintiffs' Motion for Preliminary Injunction in *Klayman II*. *Klayman v. Obama*, 957 F. Supp. 2d 1, 9-10 (D.D.C 2013). The District Court entered an order "that (1) bars the Government [Defendants] from collecting, as part of NSA's illegal government surveillance of bulk telephony metadata, any telephony metadata associated with their personal Verizon accounts and (2) requires the Government [Defendants] to destroy any such metadata in its possession that was collected through the "illegal government surveillance." App. 43. The District Court stayed its order pending appeal. App. 587.

The Government Defendants filed a notice of appeal on January 3, 2014. Under 28 U.S.C. § 1292(a)(1), this Court has appellate jurisdiction to review the District Court's order partially granting and partially denying injunctive relief.

ISSUES PRESENTED FOR REVIEW

Incorporated by reference from Appellees/Cross-Appellants initial appellate brief.

STATEMENT OF THE CASE

Incorporated by reference from Appellees/Cross-Appellants initial appellate brief.

STATEMENT OF FACTS AND PROCEDURAL HISTORY

Incorporated by reference from Appellees/Cross-Appellants initial appellate brief.

SUMMARY OF THE ARGUMENT

Incorporated by reference from Appellees/Cross-Appellants initial appellate brief.

STANDARD OF REVIEW

This Court “review[s] a District Court's weighing of the four preliminary injunction factors and its ultimate decision to issue or deny such relief for abuse of discretion.” *David v. Pension Ben. Guar. Corp.*, 571 F.3d 1288, 1291 (D.C. Cir. 2009) “Legal conclusions—including whether the movant has established irreparable harm—are reviewed *de novo*.” *Id.*

STATUTES AND REGULATIONS

All applicable statutes and regulations are contained in Appellees/Cross-Appellants' opening brief.

ARGUMENT

Specifically, the Court asked how Appellees/Cross-Appellants' Fourth Amendment rights were being violated when the Government Appellants-Cross-Appellees represented that they had not accessed their calls beyond the mere collection of telephonic metadata.

First, Appellees/Cross-Appellants have submitted affidavits (all included in the appendix) which make a prima facie showing that their specific telephonic communications are being accessed and manipulated by the Government Appellants/Cross-Appellees. *See* Exhibit 1 – Affidavits of Larry Klayman (A98), Charles Strange (A101), and David Siler (A572).

Mr. Strange swore to the following trouble with his phone and computer:

Various other contacts of mine have received text messages that seemingly appear to have been sent from my phone number, even though I had never sent said messages. Strange Affidavit ¶15, A103.

Since my son's death, I have received numerous text messages from indiscriminate numbers, all with one, two,

three, four, or five digits. I called Verizon various times and its employees stated that there is no record of the text messages being received or sent. Strange Affidavit ¶16, A103.

In July of 2013, my wife was on the computer when it abruptly photographed her face (through some form of abusive surveillance as my computer does not have a built-in camera), and falsely accused my wife of violating "Copyright and Related Rights Law". Without a built-in camera, a computer user cannot take a picture of him or herself. I have reason to believe that the NSA and other Defendants were behind this as well. Strange Affidavit ¶17, A103.

Appellees/Cross-Appellants also submitted the affidavit of David Siler, a computer expert who aided in the troubleshooting of a computer owned by Charles and Mary Ann Strange that began malfunctioning, as shown above, after they were given a disc by the Government Appellants-Cross-Appellees regarding the death of their son Michael Strange. Mr. Siler found that: "During my trouble shooting of the workstation, I found multiple viruses, spyware and keystroke loggers that had been installed on the workstation on the same date and time that Charles Strange had given me as the time he inserted the disc into his computer to view the crash report." Siler Affidavit ¶12, A573. Mr. Siler concluded by stating that "It is my professional opinion that the viruses, malware and keystroke loggers originated

from the disc drive and not the workstation and were intended by the government to access and thus violate the privacy and other rights of Charles Strange.” Siler Affidavit ¶15, A574.

Further, Appellees/Cross-Appellant Larry Klayman submitted an affidavit stating similar government activity. Mr. Klayman stated: “In fact, increasingly concerning and illegal is the fact that various contacts of mine have received text messages generated by the Defendants of this case that purport to have been sent from my cell phone number, even though I had never sent these messages.” Klayman Affidavit ¶11, A100.

Government Appellants-Cross-Appellees have never sought to refute this uncontroverted evidence. Instead, they simply represent that neither the lower court nor this Court are entitled to know what it is they are doing much less Appellees/Cross-Appellants. As Judge Richard J. Leon wrote in his Order of December 16, 2013, this “Catch-22” underscores the lack of veracity and good faith of the Government Appellants-Cross-Appellees. Without any proof provided by the Government Appellants-Cross-Appellees, the lower court and this Court are being asked to take the Government Appellants-Cross-Appellees

boldfaced and unsubstantiated assertions on face value. These assertions are demonstratively false based upon what the National Security Agency's ("NSA") own Inspector General has uncovered, which document the systematic, widespread violation of minimization procedures, namely the NSA has routinely accessed individuals identifies and metadata without probable cause to do so. The Government Appellants-Cross-Appellees were only forced to come clean with this pattern of illegal and unconstitutional conduct after whistleblower Edward Snowden revealed their ongoing criminal activity.

For example, below are just a few excerpts from the Inspector General's report, and even from the FISC Court itself, documenting this pattern of systematic abuse:

As stated in his report, the Inspector General found that:

During the investigation of alleged improprieties at NSA Georgia (NSAG) in 2004 and 2005 and reported by a former NSA assignee in 2008, we identified some practices in [redacted] that are inconsistent with established NSA/CSS policies and procedures. IG Report, Office of the Inspector General, NSA, CSS, Mem. For Commander, NSA/CSS Georgia, dated Oct. 2, 2009 at 1 (Exhibit 2).

Moreover, the FISC Court found:

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 [records] 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 misrepresentation 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.' . . . The Court concluded the [their] requirement had been 'so frequently and systematically violated that it can fairly be said that this critical element of the overall . . . regime has never functioned effectively.' FISC Memorandum Opinion at 16 n.14 (Exhibit 3).

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. FISC Memorandum Opinion at 17 n.15.

[B]ecause the alert list included all identifiers (foreign and domestic) that were of interest to counterterrorism analysts who were charged with tracking [redacted] most of the telephone identifiers compared against the incoming BR metadata were not RAS-approved. FISC Order, No. BR 08-13, at 4. The NSA "has on a daily basis, accessed the BR

metadata. . . . Such access was prohibited by the governing minimization procedures under each of the relevant Court orders, as the government conceded in its submission.” FISC Order, No. BR 08-13, at 5. FISC Order, No. BR 08-13, at 5. (Exhibit 4).

NSA has on a daily basis, accessed the BR metadata for purposes of comparing thousands of non- RAS approved telephone identifiers on its alert list against the BR metadata in order to identify any matches. Such access was prohibited by the governing minimization procedures under each of the relevant Court orders, as the government concedes in its submission, Feb. 17,2009 Memorandum at 16. FISC Order, No. BR 08-13, at 5.

The government has compounded its non-compliance with the Court's orders by repeatedly submitting inaccurate descriptions of the alert list process to the FISC. Due to the volume of U.S. person data being collected pursuant to the Court's orders, the FISC's orders have all required that any renewal application include a report on the implementation of the Court's prior orders, including a description of the manner in which the NSA applied the minimization procedures set forth therein. See. e.g., BR 08-13, Primary Order at 12. FISC Order, No. BR 08-13, at 6.

Regardless of what factors contributed to making these misrepresentations, the Court finds that the government's failure to ensure that responsible officials adequately understood the ,NSA's alert list process, and to accurately report its implementation to the Court, has prevented, for more than two years, both the government and the FISC from takin~ steps to remedy daily violations of the minimization procedures set forth in FISC orders and designed to protect [redacted] call detail records pertaining to telephone communications of U.S. persons located within the United States who are not the subject of any FBI investigation and whose call detail information could not

otherwise have been legally captured in bulk. FISC Order, No. BR 08-13, at 8-9.

The minimization procedures proposed by the government in each successive application and approved and adopted as binding by the orders of the FISC have been so frequently and systemically violated that it can fairly be said that this critical element of the overall BR regime has never functioned effectively. FISC Order, No. BR 08-13, at 11.

To approve such a program, the Court must have every confidence that the government is doing its utmost to ensure that those responsible for implementation fully comply with the Court's orders. The Court no longer has such confidence. FISC Order, No. BR 08-13, at 12.

However, the Court is very disturbed to learn that this ongoing exercise has identified additional violations of the Court's orders, including the routine accessing of BR metadata from May 2006 to February 18, 2009, through another NSA analytical tool known as [redacted] using telephone identifiers that had not been determined to meet the reasonable articulable suspicion standard. FISC Order, No. BR 08-13, at 13-14.

The record before the Court strongly suggests that, from the inception of this FISA BR program, the NSA's data accessing technologies and practices were never adequately designed to comply with the governing minimization procedures. From inception, the NSA employed two FISC Order, No. BR 08-13, at 14-15.

Under these circumstances, no one inside or outside of the NSA can represent with adequate certainty whether the NSA is complying with those procedures. In fact, the government acknowledges that, as of August 2006, "there was no single person who had a complete understanding of

the BR FISA system architecture." FISC Order, No. BR 08-13, at 15.

However, except as authorized below, the Court will not permit the government to access the data collected until such time' as the government is able to restore the Court's confidence that the government can and will comply with previously approved procedures for accessing such data. FISC Order, No. BR 08-13, at 18.

Further, the Government Appellants-Cross-Appellees have claimed that metadata does not contain and that they do not access without probable cause information about peoples' identities. In their Appellant's Brief, the Government Appellants-Cross-Appellees falsely stated that: "The governing Foreign Intelligence Surveillance Court orders require specified telecommunications companies to turn over only limited information from their business records under Section 215; that telephony metadata does not include the identity of any particular subscriber or called party." Brief of Appellants-Cross-Appellees at pp. 56 citing A203. However, this has been shown to be a complete falsehood. For example, NSA Inspector General George Ellard found that since 2003, there have been "12 substantiated instances of intentional misuse" of "surveillance authorities." About all of these cases involved an NSA employee spying on a girlfriend, boyfriend, or

some kind of love interests. Jake Gibson, *“Too tempting? NSA watchdog details how officials spied on love interests,”* FOX News (Sept. 27, 2013), available at <http://www.foxnews.com/politics/2013/09/27/too-tempting-nsa-details-how-officials-spied-on-love-interests> (Exhibit 5). More frightening, if lower level employees are capable of such misuse of the agency’s surveillance power, then imagine what the higher officials are capable of, with access to such surveillance programs.

Even more, as The Washington Post has reported, an internal audit of the National Security Agency has broken privacy rules or overstepped its legal authority thousands of times each year since 2008. See Barton Gellman, *NSA broke privacy rules thousands of times per year, audit finds*, Washington Post (August 15, 2013), available at http://www.washingtonpost.com/world/national-security/nsa-broke-privacy-rules-thousands-of-times-per-year-audit-finds/2013/08/15/3310e554-05ca-11e3-a07f-49ddc7417125_story.html (Exhibit 5). As stated by this article, “The NSA audit obtained by The Post, dated May 2012, counted 2,776 incidents in the preceding 12 months of unauthorized collection, storage, access to or distribution of legally protected communications. “ *Id.* The report continued by stating

that “the more serious lapses include unauthorized access to intercepted communications, the distribution of protected content and the use of automated systems without built-in safeguards to prevent unlawful surveillance.” *Id.*

It is clear that this Court should not believe anything that the Government Appellants/Cross-Appellees say. They are holding all of the cards and pretending as though they have safeguarded the rights of Americans when in fact every time there is leak of information the exact opposite has been shown to be true.

Further, it is black letter law that a pattern of illegal conduct will give rise to a strong evidentiary inference that unconstitutional behavior is occurring against Appellees/Cross-Appellants, particularly in the absence of any concrete direct evidence submitted by the Government Appellants-Cross-Appellees. For example, the Supreme Court case of *City of Los Angeles v. Lyons* involved repetitive unlawful conduct that gave rise to evidentiary inferences of unlawful behavior. *See City of Los Angeles v. Lyons*, 461 U.S. 95 (1983). In *Lyons*, the Supreme Court only denied the plaintiffs’ ability to sue because of their failure to establish a sufficient likelihood of future injury, which

Appellees/Cross-Appellants here have been able to demonstrate. *See id.* Other courts have also ruled that a pattern of illegal conduct may give rise to a strong evidentiary inference of unconstitutional behavior against a plaintiff. *See LaDuke v. Nelson*, 762 F.2d 1318 (9th Cir. 1985).

An evidentiary inference may also arise from third-party conduct of a pattern of similar violations of law. *See Thompson v. North American Stainless, LP*, 562 U.S. 170 (2011). As shown above, Appellants/Cross-Appellees have engaged in such a long pattern of violative conduct such that a strong evidentiary inference can be made concerning the matters at issue, that Appellants/Cross-Appellees have also violated Appellees/Cross-Appellants rights. *See also Myers v. Hodges*, 53 Fla. 197 (1907); *Abram v. Odham*, 89 So.2d 334 (1956) (evidentiary inferences in these cases show malice in defamation cases, arising from a pattern and practice of similar conduct). Thus, the Government Appellants/Cross-Appellees pattern of violative behavior detailed by the IG and the NSA's own audit, as also found by the FISC, creates a strong evidentiary inference that they have also violated Appellees/Cross-Appellants' constitutional rights. *See id.*

In short, given Appellees/Cross-Appellants' affidavits and the Government Appellants-Cross-Appellees pattern of illegal and unconstitutional conduct, this Court must conclude that Appellees/Cross-Appellants' Fourth, First and Fifth Amendment rights have been violated and affirm that Judge Leon's ruling that Appellees/Cross-Appellants indeed have standing.

As briefly discussed at the oral argument of November 4, 2014, the very nature of telephonic metadata shows that the mere collection of this information by the Appellants-Cross-Appellees itself violates at least the Fourth Amendment and has a chilling effect on the First Amendment as well. Appellees/Cross-Appellants' counsel called the Court's attention to the detailed affidavits of renowned computer expert Professor Edward Felten². Specifically, Appellees/Cross-Appellants' counsel pointed the Court to paragraph 18 of Dr. Felten's initial affidavit, who testified under oath, that the location of the individual is

² Professor Edward Felten is a professor of Computer Science and Public Affairs, as well as Director of the Center for Information Technology Policy at Princeton University. He has also served as a consultant/technology advisor in the field of computer science for numerous companies and has authored numerous books, journal articles, and other publications relating to computer science. Additionally, Professor Felten has testified several times before the U.S. Congress on computer technology issues. Felten Affidavit at ¶¶ 3, 5, 6.

easily ascertainable from the mere collection of the metadata. As set forth below, Dr. Felten also testifies to the uncontroverted fact that metadata is much more intrusive and violative of privacy than a pen register or trap and trace device.

The information sought from Verizon also includes the “trunk identifier” of telephone calls. This provides information about how a call was routed through the phone network, which naturally reveals information about the location of the parties. For example, even if the government never obtains cell site location information about a call trunk identifier information revealing that a domestic call was carried by a cable from Hawaii to the mainland United States will reveal that the caller was in the state of Hawaii at the time the call was placed. Felten Affidavit ¶ 18; A306.

Although this metadata might, on first impression, seem to be little more than “information concerning the numbers dialed,” analysis of telephony metadata often reveals information that could traditionally only be obtained by examining the contents of communications. That is, metadata is often a proxy for content. Felten Affidavit ¶ 39; A314.

Analysis of metadata on this scale can reveal the network of individuals with whom we communicate—commonly called a *social graph*. By building a social graph that maps all of an organization’s telephone calls over time, one could obtain a set of contacts that includes a substantial portion of the group’s membership, donors, political supporters, confidential sources, and so on. Analysis of the metadata belonging to these individual callers, by moving one “hop” further out, could help to classify each one, eventually yielding a detailed breakdown of the organization’s associational relationships. Felten Affidavit ¶ 48; A317.

In short, aggregated telephony metadata allows the government to construct social graphs and to study their evolution and communications patterns over days, weeks, months, or even years. Metadata analysis can reveal the rise and fall of intimate relationships, the diagnosis of a life-threatening disease, the telltale signs of a corporate merger or acquisition, the identity of a prospective government whistleblower, the social dynamics of a group of associates, or even the name of an anonymous litigant. Felten Affidavit ¶ 58; A320.

The privacy impact of collecting all communications metadata about a single person for long periods of time is qualitatively different than doing so over a period of days. Similarly, the privacy impact of assembling the call records of every American is vastly greater than the impact of collecting data about a single person or even groups of people. Mass collection not only allows the government to learn information about more people, but it also enables the government to learn new, previously private facts that it could not have learned simply by collecting the information about a few, specific individuals. Felten Affidavit ¶ 64; A322.

It is important that this Court recognize that this metadata, which goes far beyond pen registers and trap and trace devices, has been and continues to be seized not just with regard to Appellees/Cross-Appellants but hundreds of millions of Americans who are similarly situated. Even more egregiously, the metadata is being seized without any showing being made of a reasonable suspicion that is, probable cause, that these persons are communicating with terrorists or terrorist

groups much less committing a crime. In addition, the records which are being seized are not of short term duration as was true in *Smith v. Maryland*, 442 U.S. 735 (1979), but in fact go back at least five years and are updated on a daily basis. While the Government disingenuously claims that the FISC is good for only ninety days, the practice of the government has been to renew the authorizations. Thus, the unconstitutional seizure of the telephonic metadata of Appellees/Cross-Appellants and nearly all Americans continues at infinitum. As a result, hundreds of millions if not trillions of metadata is amassed by the Government Appellants-Cross-Appellees and this amounts to the most egregious violation of constitutional rights in American history such that judge Leon found himself constrained to label it “Orwellian.” Such abuse cannot be allowed to continue.

Finally, Appellees/Cross-Appellants respectfully request that this Court consider the recent Supreme Court case of *Riley v. California*, 134 S.Ct. 2473 (2014), which is analogous to this case. In *Riley*, the Court reasoned that a search of a cell phone is not the same as a very limited search of a pen register or a trace and trap and in any event, a cell phone stores a huge amount of data, and other tangible things, over a

long period of time. A pen register or trap and trace device is very limited in time and are tied to a particular crime generally. Cell phones are analogous to telephonic metadata insofar as metadata collects information under Section 215 over a five year period of time and in practice indefinitely into the future, as FISC orders are renewable every ninety days as the Government Appellants-Cross-Appellees were forced to concede at oral argument.

Chief Justice Roberts, writing for the Court, found that “[M]odern cell phones are not just another technological convenience. With all they contain and all they may reveal, they hold for many Americans “the privacies of life[.]” *Id.* at 2494. The Supreme Court also recognized that “more substantial privacy interests are at stake when digital data is involved” because “cell phones can store millions of pages of text, thousands of pictures, or hundreds of videos. . . . [which] [have] several interrelated privacy consequences.” *Id.* at 2478. Chief Justice Roberts even found that “modern cell phones . . . are now such a pervasive and insistent part of daily life that the proverbial visitor from Mars might conclude they were an important feature of human anatomy.” *Id.* at 2484

In further discussing the relevance of cellular data when it is unlawfully searched by the Government, the Supreme Court held that “a search of digital information on a cell phone does not further [] government interests . . . and implicates substantially greater individual privacy interests than a brief physical search.” *Id.* at 2478. Due to the highly sensitive data located in our cell phones, the Supreme Court made it clear that a warrant is generally required before a search, even when a cell phone is seized incident to arrest. *Id.* at 2495. Because “[d]igital data stored on a cell phone cannot itself be used as a weapon” and “can endanger no one,” the Appellants/Cross-Appellees do not have a compelling reason to search citizens’ telephony and internet metadata at their discretion. *See id.* at 2485.

CONCLUSION

For the aforementioned reasons, Appellees/Cross-Appellants submits this supplement to aid this Court in reaching its ultimate decision. This Court’s decision will have a huge impact on the constitutional rights of not just Appellees/Cross-Appellants but all Americans.

Dated: November 7, 2014

Respectfully Submitted,

/s/ *Larry Klayman*

Larry Klayman, Esq.

D.C. Bar No. 334581

2020 Pennsylvania Ave. NW #345

Washington, DC 20006

Tel: (310) 595-0800

Email: leklayman@gmail.com

CERTIFICATE OF COMPLIANCE WITH FEDERAL RULE OF
APPELLATE PROCEDURE 32(A)

I hereby certify that that this brief complies with the requirements of Federal Rule of Appellate Procedure 32(a)(5) and (6) because it has been prepared in 14-point Century Schoolbook, a proportionally spaced font.

I further certify that this brief complies with the type-volume limitation of Federal Rule of Appellate Procedure 32(a)(7)(B) because it contains 3,977 words excluding the parts of the brief exempted under Rule 32(a)(7)(B)(iii), according to the count of Microsoft Word.

/s/ Larry E. Klayman
LARRY E. KLAYMAN, ESQ.

CERTIFICATE OF SERVICE

I hereby certify that on November 7, 2014, I electronically filed the foregoing Supplemental Brief with the Clerk of the Court for the United States Court of Appeals for the District of Columbia Circuit by using the appellate CM/ECF system. I further certify that I will cause 7 paper copies of this Supplemental Brief to be filed with the Court.

Respectfully Submitted,

/s/ Larry Klayman

Larry Klayman, Esq.

D.C. Bar No. 334581

2020 Pennsylvania Ave. NW #345

Washington, DC 20006

Tel: (310) 595-0800

Email: leklayman@gmail.com

Exhibit 1

**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

AFFIDAVIT OF LARRY KLAYMAN

1. My name is Larry Klayman, I am over 18 years old. I am an adult citizen of the United States and I am the Plaintiff in the above styled case. I have personal knowledge of the facts stated in this declaration.
2. I am an attorney licensed to practice in Florida and in the District of Columbia. I am also the Founder, Chairman and General Counsel of Freedom Watch, a public interest organization dedicated to preserving civil and individual liberties and freedoms. Such advocacy includes pursuing matters related to national security, government transparency, addressing constitutional violations by the government including issues related to freedom of speech, freedom of religion, voting rights, due process rights, and other protected liberties.
3. I have been a subscriber and user of Verizon Wireless for my cellular phone service for many years and have been a subscriber and user of Verizon Wireless at all material times. I am also a user of internet services by Apple, Microsoft, YouTube, Yahoo, Google, Facebook, AT&T, and Skype and have been users of these services at all material times. I routinely

communicate with members of the public as well as journalists and associates by telephonic communications and electronic messages through Facebook, Google, Apple, and Skype.

4. I have gained public exposure and recognition through bringing numerous high profile lawsuits and strong public advocacy in matters involving public concern and public interests.

See www.freedomwatchusa.org.

5. As part of my work, and as part of Freedom Watch, I routinely communicate by telephone with existing and potential clients, whistleblowers, and other confidential sources of government abuse and corruption about their legal and other representation and discuss confidential issues, which constitute legally privileged attorney-client and other privileged communications regarding ongoing legal and other proceedings and potential proceedings.

6. I have filed the first two lawsuits against the National Security Agency, seeking to prevent them from pursuing their unconstitutional surveillance of the American people.

7. Because of my filing of these lawsuits, I have become a prime target for the NSA as I am now of the leaders of the opposition to their unconstitutional surveillance programs.

8. I am also an organizer of the growing "Reclaim America Now" movement, to stop the growing train of government abuses and usurpation by President Barack Obama and others. See www.reclaimamericanow.net. We are currently planning to hold a large-scale demonstration at Lafayette Park in Washington, D.C on November 19, 2013, where thousands if not millions will demand the resignation of Obama and high government officials who have failed to consider and take into account the grievances of the people.

9. The NSA program at issue in this case poses a substantial threat to my ability as well as the ability of Freedom Watch to do its work, which includes legal advocacy on controversial issues.

10. Defendants' mass call-tracking surveillance program has directly and significantly impacted me and my ability to communicate via telephone, email, and otherwise, given the concern that confidential, private, and legally privileged communications will be overheard or obtained by the NSA's surveillance program, and used against me, my clients, whistleblowers, and contacts concerning government abuses and corruption.

11. In fact, increasingly concerning and illegal is the fact that various contacts of mine have received text messages generated by the Defendants of this case that purport to have been sent from my cell phone number, even though I had never sent these messages.

12. These coercive tactics are designed to compromise me, my family, and friends' security and relationships with clients, whistleblowers, and other sources of government abuse and corruption, and silence me and my legal advocacy and put me in fear of the government and its unconstitutional surveillance program that I am trying to stop.

Sworn under penalty of perjury

Dated: October 28, 2013



Larry Klayman

**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

AFFIDAVIT OF CHARLES STRANGE

1. My name is Charles Strange, I am over 18 years old. I am an adult citizen of the United States and I am the Plaintiff in the above styled case. I have personal knowledge of the facts stated in this declaration.
2. I have been a subscriber and user of Verizon Wireless for my cellular phone service for many years and have been a subscriber and user of Verizon Wireless at all material times.
3. I am also a user of internet services by Apple, Microsoft, YouTube, Yahoo, Google, Facebook, AT&T, and Skype and have been users of these services at all material times.
4. I routinely communicate with my attorneys and members of the public, as well as journalists and associates by telephonic communications and electronic messages through Facebook, Google, Apple, and Skype.
5. I am the father of Michael Strange, a cryptologist technician for the National Security Agency ("NSA") and support personnel for Navy SEAL Team VI. My son, Michael, was killed when the helicopter he was in was attacked and shot down by terrorist Taliban jihadists in Afghanistan on August 6, 2011.

6. Michael was assigned to Navy SEAL Team VI, was a Petty Officer, and 1st Class (Expeditionary Warfare Specialist) in the U.S. Navy.

7. Because of Michael's position with the National Security Agency, he had access to confidential NSA and military codes and other classified information. Michael knew how the NSA worked and its methods of data collection and surveillance.

8. I believe and have said publically that Michael's death was either negligently or purposely caused by the U.S. government and/or the government of Afghanistan headed by its corrupt President, Hamid Karzai.

9. My wife Mary Ann, also a plaintiff, and I have been vocal about our criticism of President Barack Obama as Commander-in-Chief, his administration, and the U.S. military regarding the circumstances surrounding the shoot down of my son's helicopter in Afghanistan, which resulted in the death of my son, four other SEAL Team VI support personnel, seventeen SEALs, five National Guardsmen, and three Air Force members. The fatal mission was code named Extortion 17.

10. My wife and I have substantial connections with Washington, D.C., as we hold press conferences in Washington, D.C. and lobby in Washington, D.C. as advocates for my son as we seek to obtain justice for him, as well as to change the policies and orders of President Obama and the U.S. military's acts and practices, which I believe contributed to my son's death.

11. Defendants' mass call-tracking surveillance program has directly and significantly impacted my wife and my abilities to communicate via telephone, email, and otherwise, given the concern that confidential and private communications will be overheard, obtained by the NSA's surveillance program, and used against me and my family's interests.

12. Since the beginning of my advocacy and pursuit of justice for my son Michael, I have experienced several instances in which I have experienced technological abnormal intrusions.

13. On one occasion, I received an email that I believed was from Michael. It turned out that the email was a hoax. I have reason to believe, based on the totality and continuing pattern of circumstances set forth herein, that the NSA and Defendants were behind it as my son Michael could not have sent it. He is dead. This intended to cause me harm, and indeed caused me severe emotional distress. Exhibit 1.

14. There have been times when I have received text messages from friends and relatives who have told me that they had never sent the messages.

15. Various other contacts of mine have received text messages that seemingly appear to have been sent from my phone number, even though I had never sent said messages.

16. Since my son's death, I have received numerous text messages from indiscriminate numbers, all with one, two, three, four, or five digits. I called Verizon various times and its employees stated that there is no record of the text messages being received or sent. Exhibit 2.

17. In July of 2013, my wife was on the computer when it abruptly photographed her face (through some form of abusive surveillance as my computer does not have a built-in camera), and falsely accused my wife of violating "Copyright and Related Rights Law". Without a built-in camera, a computer user cannot take a picture of him or herself. I have reason to believe that the NSA and other Defendants were behind this as well. Exhibit 3.

18. The secret surveillance that the government is performing on my wife and me is making me afraid to communicate with my family, friends, and other contacts. I am in fear of my safety, my family's safety, immediate bodily injury, and even death of myself, my family, and friends.

This has heightened my emotional distress and I feel I am on the verge of a nervous breakdown. I am currently undergoing psychological counseling as a result.

19. I no longer feel able to speak as freely as I wish on the phone, or through text message and email. I have been unable to speak freely with friends, family, and other contacts, whether on the phone, through texts messages, or via email.

20. These activities by the government are prohibiting my ability to associate, to lobby Congress, to be politically active, and to communicate with my attorney Larry Klayman and others at Freedom Watch. These activities are specifically diminishing my freedom of speech.

Sworn under penalty of perjury

Dated: October 28, 2013

/s/ Charles Strange
Charles Strange

Exhibit 1

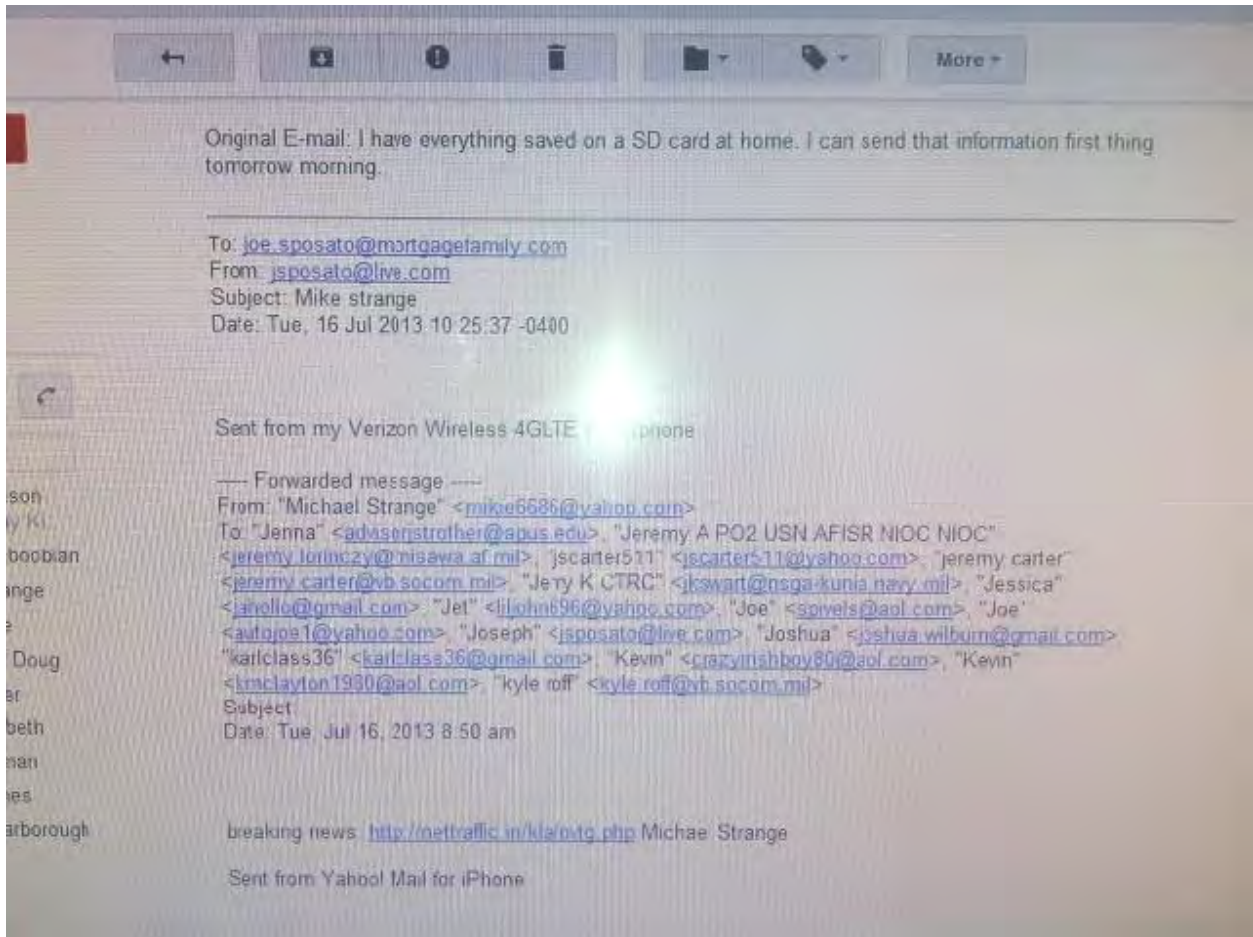


Exhibit 2

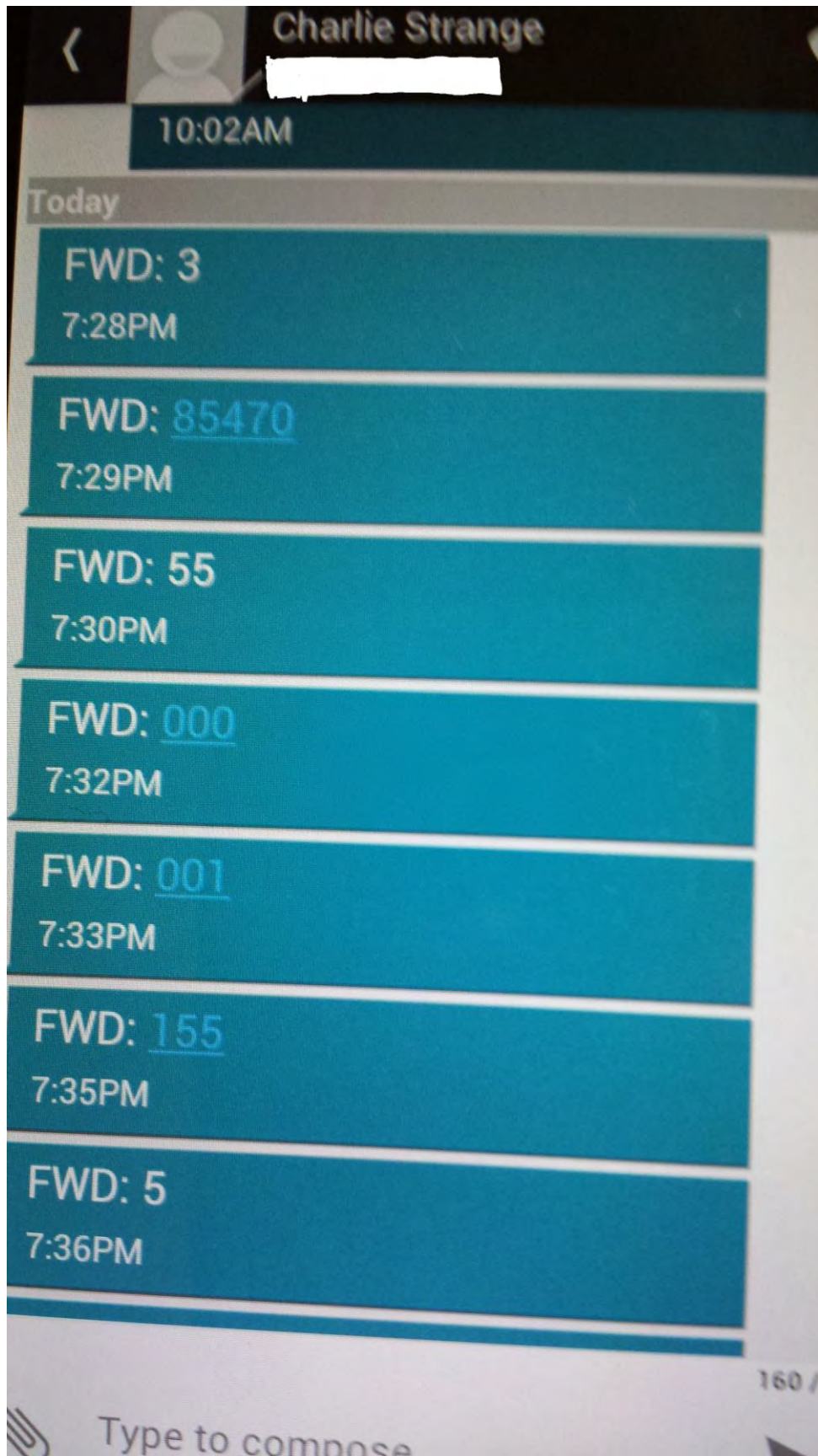


Exhibit 3

Supported and Protected by 

IP: 68.82.4.134

Location: US, United States, Pennsylvania, Philadelphia

ISP: Comcast Cable

User Name: MARY-COMPUTER



ATTENTION! Your PC is blocked due at least one of the reasons specified below.

You have been violating «Copyright and Related Rights Law» (Video, Music, Software) illegally using or distributing copyrighted content, thus infringing Article 1, Section 2, 8, also known as the Copyright of the Criminal Code of the United States of America.

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

AFFIDAVIT OF DAVID M. SILER

1. My name is David M. Siler, I am over eighteen years old. I am an adult citizen of the United States and I have personal knowledge of the facts stated in this declaration.
2. I attended Johns Hopkins University with majors in Business and Information Technologies.
3. I have been working in the computer science industry for over sixteen years.
4. I am certified in computer science in the following areas: (1) Juniper SSG 5 Firewalls; (2) NetWare 4.11 Administrator (CNA); (3) Webmaster, received from John Hopkins University; (4) A+ PC Technician; (5) Certified Juniper Networks Certified Associate; (6) Certified Dell Sonicwall Administrator
5. I currently hold over one hundred and thirty certifications granted by various hardware manufacturers.
6. As a Network Engineer and Network Administrator for multiple networks, I program and maintain Juniper, Cisco, Sonic Wall and NetGear, routers and switches, including setting up the NAT and maintaining internal and external routing tables. I configure and maintain access control and security for VPN accounts for hardware and software VPNs. I administer user's database for

domain access and accounts that include local access, OWA, and web access and recommend, configure and deploy global anti-virus and anti-spyware solutions. I am versed in a wide variety of multiple hardware platforms and maintain, install, trouble shoot, and repair any and all PC hardware.

7. Plaintiff Charles Strange informed me that he attended a debriefing held by the military on October 12, 2011 regarding his NSA-employed, cryptologist son, Michael Strange, who died when his helicopter was shot down by the Taliban on August 6, 2011 in Afghanistan.

8. Plaintiff Charles Strange informed me that on October 12, 2011 he and his wife, Mary Ann, were given a disc that contained official and redacted testimony and memoranda pertaining to the shoot-down of his son's helicopter in Afghanistan.

9. On or around April 20, 2012, Charles Strange advised me during a Vet's Journey Home Weekend that his computer was acting abnormal after he inserted the disc he was given several months earlier by the military in Dam Neck, Virginia.

10. On or around May 5, 2012, Charles Strange called me asking if I could determine what was defective with his computer. I agreed to examine the computer and Charles and his wife, Mary Ann, brought the computer to me.

11. Prior to me turning on the workstation, Charles Strange advised me of the date and approximate time he inserted the disc into his computer to view the documents that he was given by the government about his son's death.

12. During my trouble shooting of the workstation, I found multiple viruses, spyware and keystroke loggers that had been installed on the workstation on the same date and time that Charles Strange had given me as the time he inserted the disc into his computer to view the crash report.


13. I was forced to use five different tools to fully remove the viruses, malware and spyware which included Malware bytes, Combo Fix, Super AntiSpyWare, Norton Power Eraser and Kaspersky's Anti-Virus. The process took over four hours to complete.

14. After I removed the stated issues from the workstation, I then scanned the disc drive of the workstation and discovered it was infected with the installers for the viruses, malware and keystroke loggers stated above.

15. It is my professional opinion that the viruses, malware and keystroke loggers originated from the disc drive and not the workstation and were intended by the government to access and thus violate the privacy and other rights of Charles Strange.

Sworn under penalty of perjury

Dated: November 17, 2013



David M. Siler

DAVID M. SILER

dave@davesiler.com

245 North Carolina Ave
Pasadena, MD 21122
443-520-3524

Dataprise Rockville, MD

Sr. Network Engineer

April 2011 – Present

- Serving as both Sr. Network Engineer and Sr. Network Administrator on multiple networks using Windows 2000 through Windows 2012 server networks with RAID 1, 3, & 5
- Programming & maintaining Juniper, Cisco, Sonic Wall Juniper and, Netgear, routers and switches, including setting up the NAT and maintaining internal and external routing tables.
- Configuring, maintaining access control and security for VPN accounts for hardware and software VPNs
- Proposing, building, configuring and maintain MS Exchange 2003, 2007, 2010 and 2012 servers
- Proposing, building, configuring and maintaining Remote Web Workplace, OWA and 3rd party devices
- Building, servicing, and maintaining Windows 2003, 2008, 2010 & 2012 Advanced servers. Configuring Raids, and maintaining backups. (On site and with remote access.)
 - o *Managing Systems and Group Policies*
 - o *Managing and creating logon script*
 - o *Account Migrations across the domain*
 - o *Managing Trust Relationships*
 - o *Setting up and Maintaining backups using Backup Exec Ver. 9-2012*
- Administrating user's database for domain access and accounts that include local access, OWA, and web access.
- Recommending, configuring, and deploying global anti-virus and anti-spyware solutions
- Reviewing server logs and setting server policy.
- Building, installing new workstations for new employees: Including punching new CAT 5 – Cat 6 cabling, and custom building LAN cables.
- Assembling, configuring, and maintaining ESXI 5.0 based virtual server including performing P2V conversions to SAN with High Availability and failover.
- Versed in a wide variety in multiple hardware platforms ranging from Pentium 4 computers to current technologies that include up to Windows 2012 and SBS 2011 servers.
- Maintaining, installation, trouble shooting, & repair, of any and all PC hardware, printer, or business software.
- Customer relations and communications pre and post job completion.
- Completing client assessment reviews for new and current customers for recommendations of upgrades of infrastructure.

DP Solutions Columbia, MD

Network Engineer

June 2008 – April 2011

- Serving as both Network Engineer and Network Administrator on multiple networks using Windows 2000 through Windows 2008 server networks with RAID 1, 3, & 5
- Programming & maintaining Juniper, Cisco, Sonic Wall and, Netgear, routers and switches, including setting up the NAT and maintaining internal and external routing tables.
- Configuring, maintaining access control and security for VPN accounts for hardware and software VPNs
- Proposing, building, configuring and maintain MS Exchange 2003, 2007 and 2010 servers
- Proposing, building, configuring and maintaining Blackberry Enterprise Servers
- Building, servicing, and maintaining Windows 2003 & 2008 Advanced servers. Configuring Raids, and maintaining backups. (On site and with remote access.)
 - o *Managing Systems and Group Policies*
 - o *Managing and creating logon script*
 - o *Account Migrations across the domain*
 - o *Managing Trust Relationships*

- o Setting up and Maintaining backups using Backup Exec Ver. 9-12*
- Administrating user's database for domain access and accounts that include local access, OWA, and web access.
- Recommending, configuring, and deploying global anti-virus and anti spyware solutions
- Reviewing server logs and setting server policy.
- Building, installing new workstations for new employees: Including punching new CAT 5 – Cat 6 cabling, and custom building LAN cables.
- Assembling, configuring, and maintaining ESXI 4.0 based virtual server including performing P2V conversions.
- Versed in a wide variety in multiple hardware platforms ranging from 8086 computers to current technologies that include up to Windows 2008 servers.
- Maintaining, installation, trouble shooting, & repair, of any and all PC hardware, printer, or business software.
- Customer relations and communications pre and post job completion.
- Completing client assessment reviews for new and current customers for recommendations of upgrades of infrastructure.
- **Notable Mention:** Have received many thanks you emails from clients and have been in the company news letter on many occasions due to my customer service ability and client management skills.
- **Notable Accomplishments:** Tested and certified in: Juniper SA-700, IBM System x BladeCenter Technical Support V5, IBM Certified Specialist - High Volume Storage Fundamentals V,
IBM Certified Specialist - System x Technical Principles V9 and Citrix Certified Administrator for Citrix XenDesktop 4.

Americas Remote Helpdesk Eldersburg, MD

Sr. Network Engineer

October 2005 – June 2008

- Serving as both Sr. Network Engineer and Network Administrator on multiple networks using Windows Server 2000 through Windows Server 2008 networks, with RAID 1, 3, & 5
- Programming & maintaining Cisco 1700, ADSM, Cisco Catalyst Series, Sonic Walls, Netgear, routers and switches, including setting up the NAT and maintaining internal and external routing tables.
- Configuring, maintaining access control and security for VPN accounts for hardware and software VPNs
- Proposing, building, configuring Exchange 2003 Servers
- Proposing, building, configuring Blackberry Enterprise Servers
- Building, servicing, and maintaining Windows 2003 Advanced servers. Configuring Raids, and maintaining backups. (both on site and with remote access.)
 - o Managing Systems and Group Policies*
 - o Managing and creating logon script*
 - o Account Migrations across the domain*
 - o Managing Trust Relationships*
 - o Setting up and Maintaining backups using Backup Exec Ver. 9-12*
- Administrating users database for domain access and accounts that include local access, OWA, and web access.
- Recommending, configuring, and deploying global anti-virus and anti spyware solutions
- Creating, deploying, and monitoring solutions via LogMeIn scripting
- Reviewing server logs and setting server policy.
- Building, installing new workstations for new employees: Including punching new CAT 5 – Cat 6 cabling, and custom building LAN cables.
- Versed in a wide variety in multiple hardware platforms ranging from 8086 computers to current technologies, that include up to Windows 2008 server
- Maintaining, installation, trouble shooting, & repair, of any and all PC hardware, printer, or business software.
- Parts ordering for repairs: Including filling out and submitting purchase request.
- Customer relations and communications pre and post job completion.
- Completing client assessment reviews for new and current customers for recommendations of upgrades of infrastructure
- **Notable Mention:** Promoted from Network Engineer to Sr. Network Engineer within one year of employment

· **Notable Accomplishment:** Rebuild several networks migrating customers from older hardware and operation systems, to current hardware / software with very little no down time.

Art Litho Baltimore, MD

MIS Director

Jan 2004 – October 2005

- Serving as both Network Engineer and Network Administrator on a Windows NT 4.0 / Windows 2003 Server A/D Network, with RAID 1, 3, & 5, 1 PDC, 1 BDC, 1 Applications, 1 Storage, 1 Web Server, I-Mail Server, 2 FTP servers, 1 SQL Server with Active directory installed.
- Programming & maintaining Cisco 1700 series router including setting up the NAT and maintaining internal and external routing tables.
- Configuring, maintaining access control and security for dial in accounts using Shiva Land Rover.
- Building, servicing, and maintaining NT Advanced servers. Configuring Raids, and maintaining backups. (both on site and with terminal server.)
 - o *Managing Systems and Group Policies*
 - o *Managing and creating logon script*
 - o *Account Migrations across the domain*
 - o *Managing Trust Relationships*
- Administrating users database for domain access and I-Mail accounts that include local access, and web access to the account
- Reviewing server logs and setting server policy.
- Building, installing new workstations for new employees: Including punching new CAT 5 cabling, and custom building LAN cables.
- Versed in a wide variety in multiple hardware platforms ranging from 8086 computers to current technologies that include up to Windows 2003 server
- Maintaining and repairing Apple/Mac computers for Prepress department that range from OS8 to OS 10.
- Maintaining Inter-Tel phone system, voice mail, and phone assignments to current and new users. This included VOIP over a dedicated Point –to-Point T1 for a satellite office.
- Maintaining Control Access to buildings, including card key assignments, and reviewer of daily access logs.
- Maintaining, installation, trouble shooting, & repair of any and all PC hardware, printer, or business software.
- Parts ordering for repairs: Including filling out, and submitting purchase orders.
- Customer relations and communications pre and post job completion.
- Primary Software: Windows NT 4.0, Windows 2000, Windows XP, windows 2003 Server, PSI, Macola, Crystal reports, Goldmine,
- **Notable Mention:** Was awarded employee of the month award after 90 days of service due to ability to save the company over \$15K, ability to provide web access to Prepress department who had not had web access before,
and salvage of several "Non Functioning" pieces of equipment making them functional for minimal cost.
- **Notable Accomplishment:** Rebuilt entire network in 2 weeks, converting from Windows NT 4.0 Servers and workstations to Windows 2003 Server and Windows XP SP2, with NO data loss. This project included 1 PDC, 1 BDC,
1 Mail, 1 SQL Server and 30 Workstations. It also required upgrading from SQL 7.0 to SQL 2000

Popowski Brothers, Inc. Timonium, MD

Electronics Service Manager

December 2002 – October 2003

- Serving as both Network Engineer and Network Administrator on Windows 2000 Active Directory Network on a 1 RAID 5 and 1 RAID 3 and 1 TERMINAL server.
- Configuring, maintaining access control and security for dial in accounts.
- Configuring, maintaining access control and security for VPN users
- Building, servicing, and maintaining NT Advanced servers. Configuring Raids, and maintaining backups. (both on site and with terminal server.)
 - o *Managing Systems and Group Policies*

- o Managing and creating logon script*
 - o Account Migrations across the domain*
 - o Managing Trust Relationships*
- Maintaining client connectivity over 3 sites. 2 Maryland, 1 Virginia
- Administrating users database for domain access and Exchange server 5.5 accounts
- Reviewing server logs and setting server policy.
- Building, installing new workstations for new employees: Including punching new CAT 5 cabling, and custom building LAN cables.
- Versed in a wide variety in multiple hardware platforms ranging from 8086 computers to current technologies that include server
- Servicing any and all Electronic items: Including residential and commercial items.
- Providing estimates of electronic repairs to insurance adjusters and customers.
- Scheduling employee's work loads for pickups deliveries and repairs.
- Reviewing, hiring, counseling and termination, (if necessary), of employees, with the cooperation of Human Resources.
- Parts ordering for repairs: Including filling out, and submitting purchase orders.
- Customer relations and communications pre and post job completion.

Integrated Health Services Hunt Valley, MD

Sr. Desktop Analyst (1 year contract)

October 2001 to December 2002

- Developed plans for test, evaluation and deployment of software in R+D Lab.
- Designed, built, documented, and evaluated test bed for all desktop applications.
- 2nd level support for resolution of user network connectivity issues.
- Installation and usage of the following software: WSFTP, Secure CRT, Windows NT Workstation 4.0, Windows 95/98, ME, Windows 2000 Pro, MS Office 2000, Visio 2000, PaintShop Pro 7, Homesite 4.5, MS Project, Palm Software, PeopleSoft 7.06 & 8.0, Terminal Server, and many others. .
- 2nd and 3rd level support for troubleshooting and servicing any/all hardware, (computers, laptops, and printers), on site.
- Designed, Tested, Deployed, Desktop/Laptop images, for enterprise solution. (Over 270 locations Nationwide.)
- Ordering, configuring all desktops, laptops, software and licenses, as well as maintained all desktop audit info of HW/SW and license compliance.
- Designed and Implemented, Alpha & BETA, testing Project of Universal Desktop/Universal Laptop images globally, including the coordination of communication between departments for software testing phases.
- Configuration, integration, and maintenance of Windows NT 4.0 Servers, IIS Servers, and Windows 2000 Servers.
- Administration of user accounts and permissions on Windows NT/ 2000 Active Directory Servers, and MS Exchange 5.5 Servers.
 - o Managing Systems and Group Policies*
 - o Managing and creating logon script*
 - o Account Migrations across the domain*
 - o Managing Trust Relationships*

TSR, eSylvan Baltimore, MD

Network Engineer / Desktop Support Manager

March 2000 to October 2001

- Configuration, integration, and maintenance of Windows NT 4.0 Servers, IIS Servers, and Windows 2000 Servers.
- Administration of user accounts and permissions on Windows NT Servers, MS Exchange 5.5 Server, Novell 5.0 Server, and eRooms Servers.
- Developed plans for test, evaluation and deployment of software in R+D Lab.
- Designed, built, documented, and evaluated test bed for all new desktop applications.

- 2nd level support for resolution of customer network connectivity issues.
- Installation and usage of the following software: WSFTP, Secure CRT, Windows NT Workstation 4.0, Windows 95/98, ME, Windows 2000 Pro. MS Office 2000, Visio 2000, PaintShop Pro 7, Homesite 4.5, MS Project, Palm Software HelpAlert 3.6 (real time end user troubleshooting tool), network connection and monitoring tools.
- 2nd and 3rd level support for troubleshooting and servicing any/all hardware, (computers, laptops, and printers), on site.
- Managed team of technicians, determined assignment and escalation of trouble tickets, monitored progress and serving as level 3 support for desktop issues.
- Ordering, warehousing, configuring and assigning to users, all desktops, laptops, software and licenses as well as maintained all desktop audit info of HW/SW and license compliance.
- Setup and maintained desktop support helpdesk for support of internal and external users.

Key Systems **Timonium, MD**

Site Supervisor / Lead Technician

March 1999 to March 2000

- 2nd level support for resolution of customer network connectivity issues, and servicing any/all hardware, (computers and printers), on site and 2 off sight locations.
- Managed team of technicians, determined assignment and escalation of trouble tickets, monitored progress and served as level 3 support for desktop issues.
- Coordinated with networking group and telecom to have ports and / or phone extensions moved or activated as necessary.
- Installation, configuration, and usage of the following software: Windows NT Workstation, Windows 95/98, MS Office 97, Lotus Notes, Timbuktu, Remedy, Support Magic, and many other Microsoft products and operating systems.

Johns Hopkins University **Baltimore MD**
Technical Service Coordinator/Network Administrator

September 1997 to March 1999

- Network Administration functions in support of 150+ node network
- Building, Upgrading, Troubleshooting, and Administration of Novell NetWare 3.x, 4.x File Servers, Windows NT Servers, and Windows IIS Web Servers.
- Diagnosing any of the networks cabling problems for multiple Ethernet segments.
- Establishing file system security, statically assigning TCP/IP addresses, and performing regular tape backups on all the servers.
- Installation and configuration of desktops and printers attached to the network.
- Use of Altiris: Labexpert Software for scripting and imaging of single and groups of computers.
- Installation, configuration, and maintenance of server-based applications that include: IIS, War FTP, Cold Fusion, Visio, Homesite 3.0,
- MS Front Page and extensions, MS Project 98, Active Server Pages, and MS Office 97.
- Installation, configuration of all workstation software including Windows 95, Windows 98, Windows NT 4.0 Workstation, Chameleon,
- TCP/IP, Netscape Communicator, Homesite 3.0, SQL, ODBC 32, Microsoft Client for NetWare, and Novell Intranetware.
- Configuring all hardware and software upgrades.
- Installation, configuration, troubleshooting and replacing when necessary, any PC or printer hardware components. (This included SCSI and IDE hard drives, CD ROM drives, video adapters, sound cards, modems, memory modules (SIMMs), Zip drives, Jazz drives, Network Interface Cards), all printer parts.
- Provided level 3 help desk functions and support to both staff and students.
- Working directly with vendors to get parts, upgrades, and quotes for major improvements to the Center's technology.
- Provided A/V support for production sound and video of live broadcasts.

Johns Hopkins University **Baltimore, MD**

Micro Computer Technician

September 1996 to September 1997

- Provide PC and Macintosh, hardware and software support, for a network comprised of over 3000 desktops, 600 printers, and 120 file servers.
- Troubleshooting, diagnosing, and repairing all microcomputer components including, SCSI drives, SCSI controllers, NICs, video adapters, SIMMs, power supplies, and keyboards.
- Perform diagnostics, repair, upgrading and supporting of all hardware and software products, including desktops, laptops, X86s, Pentiums, Apple-Mac's, and OS/2 machines.

Computer City Glen Burnie, MD

Hardware/Software Configuration Manager

July 1994 to September 1996

- Installation, configuration, and support of any hardware and software products in a technical repair shop for a high volume retail computer store.
- Responsible for the custom build out of retail orders, involving disk drives, memory, sound systems, multimedia, and network components.
- Directly supervised four microcomputer technicians in day-to-day operations.
- Responsible for prioritizing work orders, assigning tasks, tracking repair, ordering parts for repairs, and customer support.

EDUCATION:

Johns Hopkins University (Did not receive degree)
Major: Business/Information Technologies GPA: 3.78 Credits: 6

Anne Arundel Community College (Did not receive degree)
Major: Criminal Law GPA: 3.42 Credits: 21

Certifications:

Certified Juniper SSG 5 Firewalls
Certified Sonicwall Administrator
Certified NetWare 4.11 Administrator (CNA)
Certified Webmaster: Received Jan. 27, 1999 from Johns Hopkins University
Certified A+ PC Technician
Currently holding 130+ Certifications granted by various hardware manufactures.

Certifications:

CNA

Certified Novell Administrator 4.11, Completed: March 18, 1998

A+

A+ Certificate, Completed Jan. 30, 1997

Webmaster

WebMaster Certificate, Completed: January 27, 1999

Juniper

Junos Fundamentals

The Junos Software Advantage FOUNDJUNOS260309040056

JNSA

Advanced Security

Juniper Networks Sales Associate SSL JNSASSL130609040014

Juniper Networks Sales Associate Firewall JNSAFWV120609040091

Juniper Networks Sales Associate IDP JNSAIDP130609040006

Network Infrastructure

Juniper Networks Sales Associate Enterprise Switch JNSAEX130609040020

Juniper Networks Sales Associate WAN Acceleration JNSAWX130609040023

JNSS

Advanced Security

Juniper Networks Sales Specialist SSL JNSSSSL030409040050

Juniper Networks Sales Specialist Firewall JNSSFWV260309040066

Juniper Networks Sales Specialist IDP JNSSIDP270509040082

Network Infrastructure

Juniper Networks Sales Specialist Enterprise Switch JNSSEX280509040003

Juniper Networks Sales Specialist WAN Acceleration JNSSWX280509040006

Juniper Networks Sales Specialist Enterprise Routing JNSSMMX020609040019

Technical Certifications

Juniper Networks Certified Internet Associate - Firewall/VPN November 23, 2011

Juniper Networks Certified Internet Associate - SSL April 16, 2010

Hewlett Packard

SPN: 032 - Vectra 386, 16N, 20N, 25NS, 20S, &25 PC, Completed Aug. 8, 1996
SPN: 033 - ScanJet 3P, II Series Scanners, Completed June 15, 1995
SPN: 034 - Vectra 486U PC Series, Completed Aug 8, 1996
SPN: 036 - Vectra PC Product Line Training 1992, Completed Aug. 7, 1996
SPN: 038 - Netserver LE Service, Completed May 7, 1999
SPN: 039 - Netserver LM Service, Completed May 3, 1999
SPN: 040 - Netserver LH Service, Completed April 21, 1999
SPN: 044 - NetServer LF Service, Completed May 13, 1999
SPN: 045 - Netserver LC Service, Completed May 3, 1999
SPN: 047 - Netserver LS Service, Completed April 28, 1999
SPN: 048 - 5000,7000 Home PC Series, Completed Aug. 7, 1996
SPN: 050 - Vectra 1996 Model PC Service, Completed May 21, 1999
SPN: 051 - Vectra 500 PC Service, Complete May 18, 1999
SPN: 052 - Netserver LX Service, Completed May 3, 1999
SPN: 053 - Netserver E30 Service, Completed April 21, 1999
SPN: 054 - Vectra 1997 Model PC Service, Completed May 20, 1999
SPN: 055 - Netserver E40/E45/E50 Service, Completed April 29, 1999
SPN: 057 - Netserver LC II Service, Completed June 28, 1999
SPN: 059 - 1998 Brio, Vectra, Kayak Service, Completed April 21, 1999
SPN: 060 - Netserver LH4/4r Service, Completed June 30, 1999
SPN: 061 - Netserver LXr 8000 Service, Completed June 30, 1999
SPN: 062 - Netserver LPr Service, Completed July 1, 1999
SPN: 064 - 1999 PC & PC Workstation Service, Completed June 4, 1999
SPN: 065 - Netserver E60 Service, Completed June 28, 1999
SPN: 076 - HP Workstation Products, Completed October 31, 2001
SPN: 078 - HP Pavillion Notebooks, Completed November 2, 2001
SPN: 214 - DesignJet 600 Service, Completed June 8, 1999
SPN: 216 - DesignJet 650C Service, Completed June 4, 1999
SPN: 218 - DesignJet 200 & 220 Service, Completed June 4, 1999
SPN: 219 - DesignJet 230,250C,330,350C Service, Completed June 7, 1999
SPN: 220 - DesignJet 700, 750C, 750C+, 755CM, Completed April 8, 1999
SPN: 221 - DesignJet 430/450C/455CA Service, Completed June 8, 1999
SPN: 311 - Laserjet Models 33440, 33447, 33449, 33459, Completed May 13, 1999
SPN: 312 - Laserjet IIP, IIP+, IIIP Printers, Completed Dec. 5 1994
SPN: 319 - DeskWriter C, 520,550C, &560C Diag., Completed July 31, 1995
SPN: 322 - DeskJet 500C, 520,550C, 560C Diag., Completed July 31, 1995
SPN: 325 - LaserJet 4,4M, 4Plus, & 4M Plus, Completed June 17, 1995
SPN: 326 - LaserJet IIISI, 4Si, &4SIMX, Completed June 28, 1996
SPN: 327 - LaserJet 4L, 4ML, 4P, 4MP, 5P, 5MP, Completed June 6, 1995

SPN: 328 - Deskjet 1200C,1600C, PS, Completed Sept. 19, 1995
SPN: 333 - DeskJet 540,600, Completed Sept. 7, 1995
SPN: 334 - DeskWriter 540,600C, 660C, Completed Sept. 7, 1995
SPN: 335 - Color Laserjet Printer Service, Completed April 12, 1999
SPN: 336 - LaserJet 4V-4MV, Completed June 9, 1995
SPN: 339 - Laserjet 5L & 6L Printer Service, Completed April 19, 1999
SPN: 340 - Copyjet Models C3817A & C3819A, Completed Sept. 28, 1996
SPN: 341 - LaserJet 5SI & 5SIMX, Completed June 11, 1996
SPN: 342 - Laserjet 4SI Network Scanner, Completed April 16, 1999
SPN: 343 - DeskJet 850C & 855C, Completed May 13, 1999
SPN: 344 - Network Scanjet 5 Scanner Service, Completed April 6, 1999
SPN: 346 - Laserjet 4000, 4000N, 4000TN, Completed March 24, 1999
SPN: 347 - Laserjet 5000, 5000N, 5000GN, Completed March 30, 1999
SPN: 348 - Laserjet 3100 Service, Completed May 4, 1999
SPN: 350 - Deskjet 340/340CM, Completed April 15, 1999
SPN: 352 - OfficeJet/OfficeJet LX Service, Completed June 2, 1999
SPN: 353 - OfficeJet Series 300 Service, Completed May 24, 1999
SPN: 354 - OfficeJet Pro 1150C/1170C/1175C Service, Completed June 3, 1999
SPN: 355 - Color LaserJet 4500 Service, Completed June 17, 1999
SPN: 356 - Color Laserjet 8500, 8500N, 850DN, Completed April 9, 1999
SPN: 358 - OfficeJet 500,600,700 & Print/Scan/Copy 370/380, Completed June 2, 1999
SPN: 359 - Laserjet 1100 Printer Service, Completed April 27, 1999
SPN: 361 - Laserjet 2100, Completed March 24, 1999
SPN: 362 - HP25000C/CM Color Printer Service, Completed June 11, 1999
SPN: 363 - Laserjet 3150, Completed March 2, 2000
SPN: 365 - LaserJet 8000 & 8100 MFP, Completed November 8, 2001
SPN: 412 - Optimizing Workgroup Performance, Completed April 10, 1999
SPN: 414 - JetDirect Print Servers, Completed April 8, 1999
SPN: 421 - SureStore Diagnostic Service, Completed December 8, 1999
SPN: 505 - Fax 700/750 & 900/950, Completed April 29, 1999
SPN: 604 - Omnibook Notebook PCs Laptop, Completed June 3, 1999
SPN: 605 - Omnibook 600 & 800, Completed April 29, 1999
SPN: 606 - Omnibook 3000 Service, Completed June 16, 1999
SPN: 607 - Omnibook Performance 98 Service, Completed June 18, 1999
SPN: 901 - LaserJet Basic Hardware Training, Completed Nov. 2, 1994
SPN: 995 - HP Facilitation Support, Completed November 19, 2001
SPN: 997 - Deskjet 800 Series, Completed April 30, 1999
SPN: 998 - DeskJet/Deskwriter 400, 540, 600, 600C, 720, Completed April 19, 1999
SPN: 999 - Manuals and Tests for Discount, Completed November 2, 1994

Okidata

ML590 ML 590/591 Printer Training, Completed Oct. 24, 1994
Update ML 590/591 Printer Training Update, Completed Feb. 14, 1995
ML300 ML 300 Printer Training, Completed Feb. 14, 1995
ML380 ML 380 Printer Training, Completed Feb. 14, 1995
ML395 ML 395 Printer Training, Completed Feb. 14, 1995
ML393 ML 393-Plus Printer Training, Completed Feb 14, 1995
OL400e OL 400E/410E Printer Training, Completed Feb. 14, 1995
OL400 OL 400/800/820/830/840 Printer Training, Completed Feb. 14, 1995
OL810 OL 810 Printer Training, Completed Feb. 14, 1995
OL810 OL 830-Plus/850 Printer Training, Completed Feb 14, 1995

Leading Edge

Repair of Leading Edge Computers, Completed Mar 17, 1995

Cannon

BJ200 BJ-200, 230, 200E, 100 Bubble Jet, Completed Oct 21, 1994
BJ600 BJC-600, 600E Bubble Jet Printers, Completed Mar 27, 1995
BJ10 BJ-10 Series Bubble Jet Printers, Completed Feb 16, 1995

Dell

Dimension Desktops, Expires:04/26/2000
Dell Workstations, Expires: 04/26/2000
Latitude Notebooks, Expires: 04/26/2000
PowerEdge Servers, Expires: 04/26/2000

AST

8000 Advantage 8000 PC, Completed Apr 13, 1996
Cupid Cupid Desktop PC, Completed May 26, 1995
Bravo Bravo Family PC, Completed Aug 21, 1996

Lexmark

4076 OWJ Service Training, Completed Aug 1996
4076-02C Service Training, Completed Aug 1996
4077 (Winwriter 150C) Service Training, Completed Aug 1996
4090 Color Jetprinter 2070 Training, Completed Aug 1996
4076 Color Jetprinter Service Training, Completed Aug 1996

4078 Color Jetprinter Service Training, Completed Aug 1996

IBM

IBM Certified Specialist- System x Technical Principles V9 - May 3, 2010

IBM Certified Specialist- High Volume Storage Fundamentals V1 - May 12, 2010

IBM Certified Specialist- BladeCenter Technical Support V5 - May 18, 2010

PS Server Service Training, Completed Jan. 1996

PS Server Service Training Update, Completed Mar. 1996

PS Server 500 Service Training, Completed Feb. 1996

PS Server Line Ver. 2 Service Training, Completed Mar. 1996

ThinkPad Service Training, Completed Sept. 1995

Network Printer 12 Service Training, Completed Apr. 1995

Network Printer 17 Service Training, Completed May 1996

Warranty Support &PS/ ValuePoint, Completed Dec. 1995

PS/2 Micro Channels Models, Completed Nov. 1995

Warranty Basics Service Training, Completed Oct. 1995

Warranty Basics Service Training Update, Completed Mar. 1999

Network Color Printer Service Training, Completed Apr. 1996

Mobile Systems Training, Completed Mar. 1999

Desktop Systems Repair Training, Completed Mar. 1999

Exhibit 2

~~SECRET//REL TO USA, FVEY~~



OFFICE OF THE INSPECTOR GENERAL
NATIONAL SECURITY AGENCY
CENTRAL SECURITY SERVICE

October 2, 2009

IG-11084-09

(U) MEMORANDUM FOR COMMANDER, NSA/CSS GEORGIA,
Fort Gordon, GA

(U//~~FOUO~~) OFFICER IN CHARGE (OIC), [redacted] NSA/CSS
GEORGIA, Fort Gordon, GA

SUBJECT: (U//~~FOUO~~) Intelligence Oversight of the [redacted]
Program at NSA/CSS Georgia (ST-09-0020) - ACTION MEMORANDUM

(b) (3) - P.L. 86-36

(U//~~FOUO~~) During the investigation of alleged improprieties at NSA Georgia (NSAG) in 2004 and 2005 and reported by a former NSA assignee in 2008, we identified some practices in [redacted] that are inconsistent with established NSA/CSS policies and procedures. For details concerning the investigation, see *Report of Investigation Regarding Alleged Improprieties at NSA Georgia* (Report of Investigation), IV-09-0003, August 14, 2009. These practices may increase the risk of mishandling U.S. persons information and, therefore, require your attention.

A. (U) Improper Dissemination of Raw SIGINT

~~(S//REL TO USA, FVEY)~~ We discovered that as of 20 August 2009,

[redacted] Daily Summaries could be accessed in [redacted] archives on NSAnet.¹ For a listing of the summaries, see pp. 30 - 34 in the Report of Investigation. The [redacted] Daily Summaries were also saved in the Extended Shared Enterprise Corporate Server (ESECS).² These summaries or gists are not minimized for dissemination and are, therefore, considered raw traffic. They can be viewed by anyone with an NSAnet account, including personnel outside the SIGINT production chain, thus constituting

(b) (1)
(b) (3) - P.L. 86-36
(b) (3) - 18 USC 798
(b) (3) - 50 USC 3024 (i)

~~(S//REL TO USA, FVEY)~~ [redacted] Daily Summaries are created from data pulled by analysts [redacted]

² (U//~~FOUO~~) ESECS is a web-based collaboration suite or content management system hosted on NSAnet that provides workflow automation, document management, content search, and subscription/notification services. It provides communities of interest in which organizations can store information and share it among their analysts and with their customers. Most content within ESECS is viewable by the entire user population; however, access policies can be applied to any object to restrict access.

Derived From: NSA/CSSM 1-52

Dated: 20070108

Declassify On: 20340401

~~SECRET//REL TO USA, FVEY~~

~~SECRET//REL TO USA, FVEY~~

dissemination. Such access to raw traffic is inconsistent with USSID SP0018, § 6.2, which requires that access to raw traffic storage systems containing identities of U.S. persons be limited to SIGINT production personnel. As a result, [redacted] should develop: 1) written procedures for properly reviewing materials so that only evaluated and minimized traffic is posted on [redacted] NSAnet website; and 2) access controls to ensure that only authorized personnel within the SIGINT production chain gain access to unminimized SIGINT, [redacted]

(b) (1)
(b) (3)-P.L. 86-36

(b) (1)
(b) (3)-P.L. 86-36
(b) (3)-18 USC 798
(b) (3)-50 USC 3024(i)

B. (U) Retention Period of U.S. Persons Information

(U//~~FOUO~~) In accordance with USSID SP0018, § 6.1.a, NSAG should assess the need to retain the summaries containing U.S. person information addressed in the Report of Investigation. [redacted]

[redacted]

(b) (3)-P.L. 86-36

(U//~~FOUO~~) [redacted]

[redacted]

C. (U) Noncompliance with Quarterly Reporting Requirements

(U//~~FOUO~~) Although [redacted] currently provides informal input (by email, with no [redacted] OIC review) for the NSAG Quarterly Report on Compliance with E.O. 12333 and Related Directives, this reporting does not meet the standard in USSID SE5120, which states:

3.6. (C//REL) [redacted] will submit a quarterly report via NSA/CSS Georgia to the Office of Inspector General (OIG) of activity covered by Executive Order 12333 (*emphasis added*).³

(b) (1)
(b) (3)-P.L. 86-36
(b) (3)-18 USC 798
(b) (3)-50 USC 3024(i)

(b) (3)-P.L. 86-36

(U//~~FOUO~~) The informal process used by NSAG to obtain [redacted] input for the Quarterly Report does not ensure complete reporting and gives both [redacted] and NSAG only limited visibility into [redacted] compliance. In accordance with USSID SE5120 and NSA guidance, [redacted] should prepare a complete and formal report, signed by the [redacted] OIC, thereby certifying appropriate

³ The USSID mirrors standards in Paragraph 8.4 in USSID SP0018 and Paragraph 7.g. in NSA/CSS Policy 1-23.

~~SECRET//REL TO USA, FVEY~~

~~SECRET//REL TO USA, FVEY~~

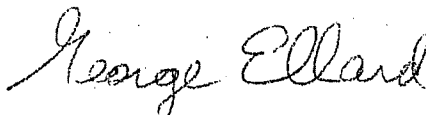
oversight of intelligence activities. The OIC is responsible for ensuring that [] SIGINT activities are lawful and not contrary to SIGINT authorities and that employees are aware of the authorities as they relate to the [] mission. NSAG should maintain copies of [] reports for review by oversight officials upon request.

(b) (3) - P, L, 86-36

(U//FOUO) We also noted that, in 2004 and 2005, [] IO training was not uniform for all personnel performing the [] mission and did not adhere to the standards set in NSA/CSS policies.⁴ In 2006, NSAG changed its IO training standards so that all personnel receiving an NSAG badge must complete NSAG IO training upon initial assignment and annually thereafter. Additionally, [] now uses Job Qualification Standards for linguists and analysts that all newly-assigned personnel must successfully complete. These procedures were not reviewed during the investigation, but will be evaluated during the upcoming Joint Inspection of NSAG scheduled for February 2010.

(U//FOUO) We request that NSAG, with the assistance of the [] provide us with a status of actions taken to resolve the aforementioned inconsistencies. We appreciate the courtesy and cooperation extended to the investigators throughout the investigation. If you need clarification or additional information, please contact [] on 963-2979 (s) or by e-mail at []@nsa.

(b) (6)



GEORGE ELLARD
Inspector General

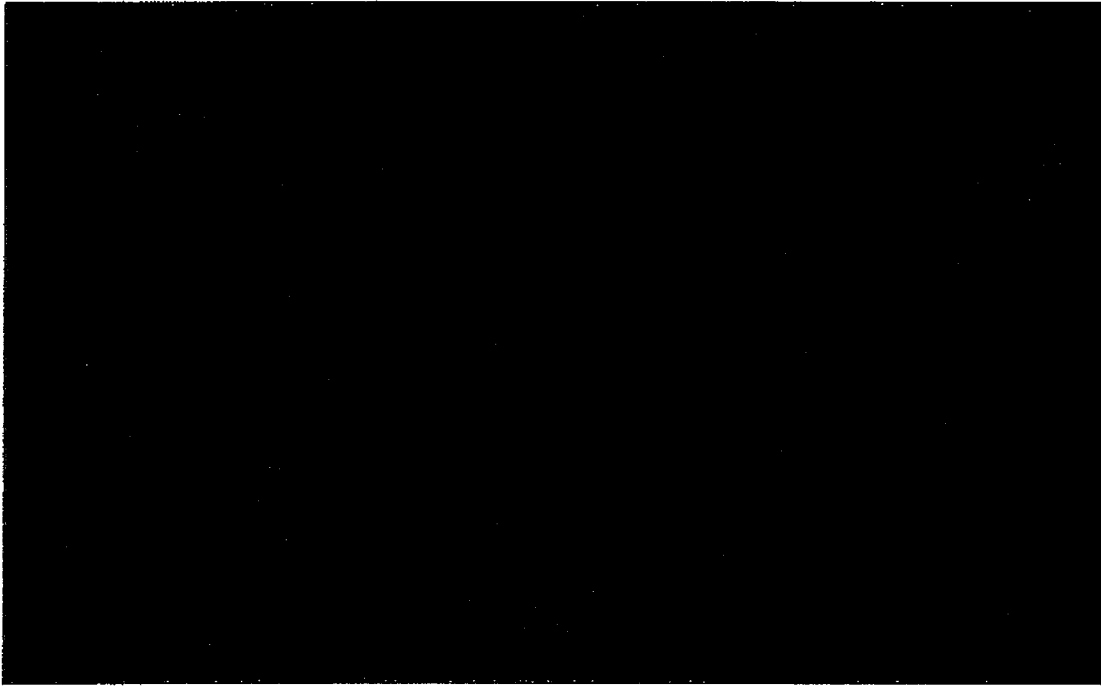
⁴ Paragraph 7.b. in NSA/CSS Policy 1-23, and Paragraph 7.4 in USSID 5762(P).

~~SECRET//REL TO USA, FVEY~~

Exhibit 3

~~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, 2011.¹

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.

¹ 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] (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.²

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

² 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]

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”³ of Internet communications includes the acquisition of entire “transaction[s]” [REDACTED]

[REDACTED]⁴ 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).

³ 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].

⁴ 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 6.⁵

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

⁵ 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").⁶

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

⁶ 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 procedures⁷ and minimization procedures;⁸

(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);⁹ and

(5) each of the certifications includes an effective date for the authorization in compliance

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

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

⁹ 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]
[REDACTED]¹⁰

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.¹¹ 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

¹⁰ 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).

¹¹ [REDACTED]

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

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

Certification [REDACTED]¹² 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),¹³ 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).

¹² 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]

¹³ 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~~

~~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~~

~~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]

[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.¹⁴

¹⁴ 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 2008,¹⁵ 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.¹⁶ The Court will

¹⁴ [REDACTED]

¹⁵ 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.

¹⁶ 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.¹⁷

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].¹⁸

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

¹⁶(...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.

¹⁷ 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.

¹⁸ 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]¹⁹ 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.²⁰

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

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

²⁰ 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.²¹ 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] 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

²¹ 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.²²

The amended CIA minimization procedures include [REDACTED]

²² 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] 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,”²³ 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

²³ 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.²⁴ Sept. 9 Submission at 1; Aug. 16 Submission at Appendix A. Indeed, NSA's upstream collection constitutes only approximately

²⁴ 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."²⁵ 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.²⁶ 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]

²⁵ [REDACTED]

²⁶ 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.²⁷ *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.²⁸ *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]

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

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

First, the Court previously understood that NSA's technical measures²⁹ 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 collection³⁰ reveals that NSA acquires approximately 2,000-10,000 MCTs each year that contain at least one wholly domestic communication.³¹ See Aug. 16 Submission at 9. In addition to these MCTs, NSA

²⁹ [REDACTED]

³⁰ 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.

³¹ 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,³² given that NSA's upstream collection devices will acquire a wholly domestic "about" SCT if it is routed internationally.³³ Moreover, the actual number of wholly domestic communications acquired

³² 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.

³³ 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~~

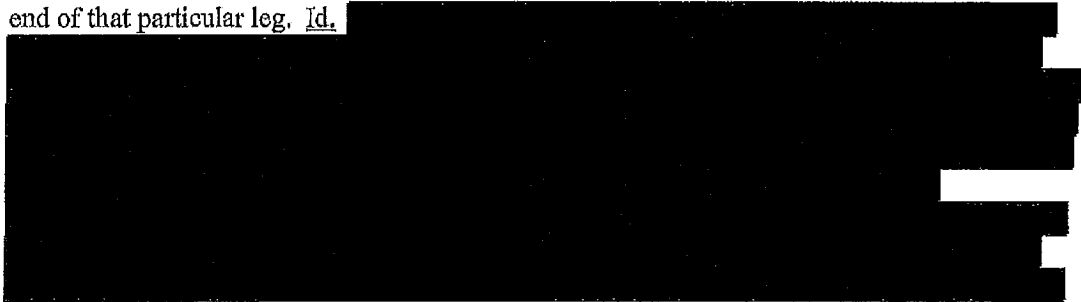
~~TOP SECRET//COMINT//ORCON,NOFORN~~

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.³⁴

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

³³(...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.*



³⁴ 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,³⁵ 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

³⁵ 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~~

~~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.³⁶

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;³⁷
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

³⁶ 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.

³⁷ 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.

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

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

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.³⁸

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

³⁸ 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.

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

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

persons in the United States.³⁹

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.⁴⁰ 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,⁴¹ so even if only 1% of these MCTs

³⁹ 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.

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

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

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

~~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.⁴² 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

⁴¹(...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.

⁴² 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~~

~~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~~

~~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]
[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~~

~~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

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

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

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

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

⁴³ 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~~

~~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]

⁴⁴ 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~~

~~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

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

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

“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 8-11.⁴⁵ 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

⁴⁵ 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.

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

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

Minimization Procedures § 3(a).⁴⁶ 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

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

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

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

information or evidence of a crime, or that it falls into another narrow exception permitting retention. See id. § 5.⁴⁷

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).⁴⁸

⁴⁷ 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.

⁴⁸ 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...)

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

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

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

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

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

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

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

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.6.⁵⁰ 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,”

⁴⁹ 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.

⁵⁰ 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~~

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

presumably by reviewing some or all of the MCT's contents. Id. at 8.⁵¹ "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 8-9.⁵² 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.

⁵¹ 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.

⁵² 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.").

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

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

- 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,⁵³ and tens of thousands of communications of or

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

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

~~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

⁵³(...continued)

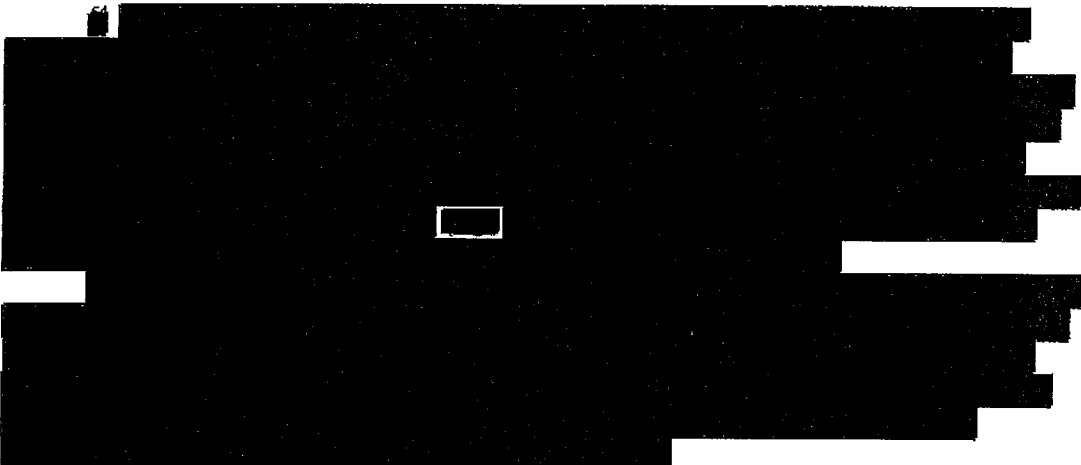
of thousands of wholly domestic SCTs that contain references to targeted selectors. See supra, pages 33-34 & note 33 (discussing the limits [REDACTED])

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 27.⁵⁴ 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~~

~~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

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

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

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).⁵⁵ 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

⁵⁵ 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.

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

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

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

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

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

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.⁵⁶ 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

⁵⁶ 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~~

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

United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information.”⁵⁷ 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).

⁵⁷ 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



. 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~~

~~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.*⁵⁸

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).⁵⁹ The government has proposed several additional restrictions that

⁵⁸ 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.

⁵⁹ 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...)"

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

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

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

⁵⁹(...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).

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

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

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.⁶⁰ 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.⁶¹ Accordingly, the Court concludes that NSA’s

⁶⁰ 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.

⁶¹ 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~~

~~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).⁶²

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

⁶² 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~~

~~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*”).⁶³ 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

⁶³ 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~~

~~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).⁶⁴

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

⁶⁴ 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.⁶⁵ In arguing that NSA’s

⁶⁵ 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~~

~~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.⁶⁶

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

⁶⁶ 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~~

~~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~~

~~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.⁶⁷

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

⁶⁷ 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~~

~~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.⁶⁸

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;

⁶⁸ 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,⁶⁹ 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.

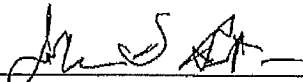
⁶⁹ See Docket No. [REDACTED]

~~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

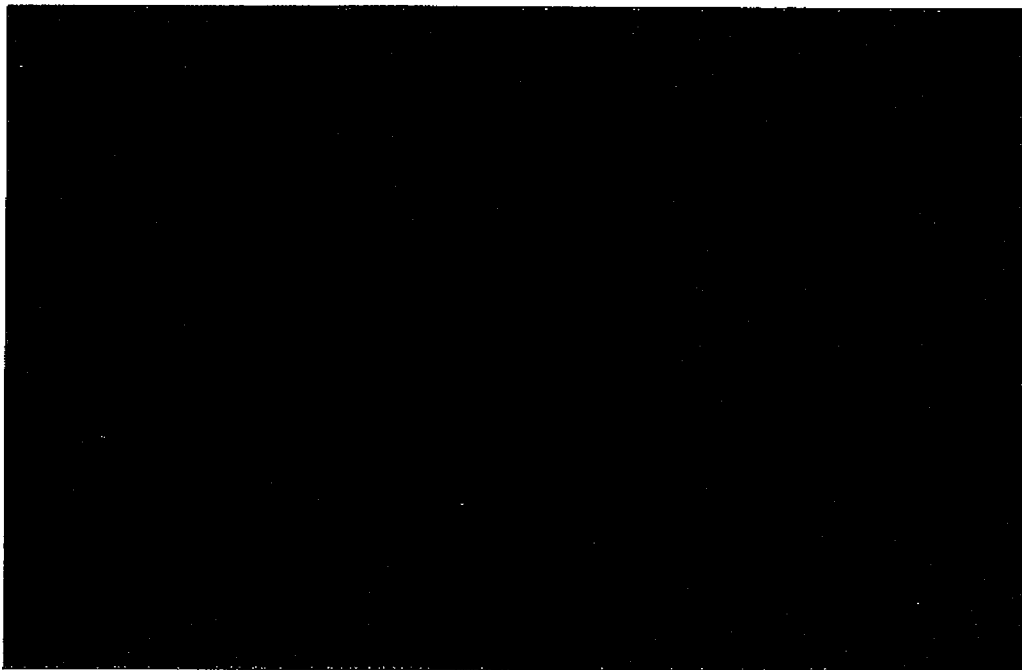
██████████, Deputy Clerk,
FISC, certify that this document
is a true and correct copy of
the original. ██████████

~~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,¹ 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,

¹ 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, [redacted] Deputy Clerk,
FISC, certify that this document
is a true and correct copy of
the original [redacted]

(b)(6)

Exhibit 4

~~TOP SECRET//COMINT//NOFORN//MR~~

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

IN RE PRODUCTION OF TANGIBLE THINGS
FROM [REDACTED]

Docket Number: BR 08-13

ORDER

On December 12, 2008, the Foreign Intelligence Surveillance Court ("FISC" or "Court") re-authorized the government to acquire the tangible things sought by the government in its application in the above-captioned docket ("BR 08-13"). Specifically, the Court ordered [REDACTED] to produce, on an ongoing daily basis for the duration of the order, an electronic copy of all call detail records or "telephony metadata" created by [REDACTED] BR 08-13, Primary Order at 4. The Court found reasonable grounds to believe that the tangible things sought are relevant to authorized investigations being conducted by the Federal Bureau of Investigation ("FBI") to protect against international terrorism, which investigations are not being conducted solely upon the basis of First Amendment protected activities, as required by 50 U.S.C. §§1861(b)(2)(A) and (c)(1). *Id.* at 3. In making this finding, the Court relied on the

~~TOP SECRET//COMINT//NOFORN//MR~~

~~TOP SECRET//COMINT//NOFORN//MR~~

assertion of the National Security Agency (“NSA”) that having access to the call detail records “is vital to NSA’s counterterrorism intelligence mission” because “[t]he only effective means by which NSA analysts are able continuously to keep track of [REDACTED]

[REDACTED] and all affiliates of one of the aforementioned entities [who are taking steps to disguise and obscure their communications and identities], is to obtain and maintain an archive of metadata that will permit these tactics to be uncovered.” BR 08-13, Application Exhibit A, Declaration of [REDACTED]

Signals Intelligence Directorate Deputy Program Manager [REDACTED]

NSA, filed Dec. 11, 2008 (“[REDACTED] Declaration”) at 5. NSA

also averred that

[t]o be able to exploit metadata fully, the data must be collected in bulk.... The ability to accumulate a metadata archive and set it aside for carefully controlled searches and analysis will substantially increase NSA’s ability to detect and identify members of [REDACTED]

Id. at 5-6.

Because the collection would result in NSA collecting call detail records pertaining to [REDACTED] of telephone communications, including call detail records pertaining to communications of United States (“U.S.”) persons located within the U.S. who are not the subject of any FBI investigation and whose metadata could not otherwise be legally captured in bulk, the government proposed stringent minimization procedures that strictly controlled the

~~TOP SECRET//COMINT//NOFORN//MR~~

~~TOP SECRET//COMINT//NOFORN//MR~~

acquisition, accessing, dissemination, and retention of these records by the NSA and the FBI.¹ BR 08-13, Application at 12, 19-28. The Court's Primary Order directed the government to strictly adhere to these procedures, as required by 50 U.S.C. 1861(c)(1). Id. at 4-12. Among other things, the Court ordered that:

access to the archived data shall occur only when NSA has identified a known telephone identifier for which, based on the factual and practical considerations of everyday life on which reasonable and prudent persons act, there are facts giving rise to a reasonable, articulable suspicion that the telephone identifier is associated with [REDACTED]

[REDACTED] provided, however, that a telephone identifier believed to be used by a U.S. person shall not be regarded as associated with [REDACTED]

[REDACTED] solely on the basis of activities that are protected by the First Amendment to the Constitution.

Id. at 8 (emphasis added).

In response to a Preliminary Notice of Compliance Incident dated January 15, 2009, this Court ordered further briefing on the non-compliance incident to help the Court assess whether its Orders should be modified or rescinded; whether other remedial steps should be directed; and whether the Court should take action regarding persons responsible for any misrepresentations to the Court or violations of its Orders. Order Regarding Preliminary Notice of Compliance Incident Dated January 15, 2009, issued Jan. 28, 2009, at 2. The government timely filed its Memorandum in Response to the Court's Order on February 17, 2009. Memorandum of the United States In Response to the Court's Order Dated January 28, 2009 ("Feb. 17, 2009

¹The Court notes that the procedures set forth in the government's application and the [REDACTED] Declaration are described in the government's application as "minimization procedures." BR 08-13, Application at 20.

~~TOP SECRET//COMINT//NOFORN//MR~~

~~TOP SECRET//COMINT//NOFORN//MR~~

Memorandum”).

A. NSA’s Unauthorized Use of the Alert List

The government reported in the Feb. 17, 2009 Memorandum that, prior to the Court’s initial authorization on May 24, 2006 (BR 06-05), the NSA had developed an “alert list process” to assist the NSA in prioritizing its review of the telephony metadata it received. Feb. 17, 2009 Memorandum at 8. Following the Court’s initial authorization, the NSA revised this alert list process so that it compared the telephone identifiers on the alert list against incoming FISC-authorized Business Record metadata (“BR metadata”) and SIGINT collection from other sources, and notified NSA’s counterterrorism organization if there was a match between an identifier on the alert list and an identifier in the incoming data. Feb. 17, 2009 Memorandum at 9-10. The revised NSA process limited any further analysis of such identifiers using the BR metadata to those telephone identifiers determined to have met the “reasonable articulable suspicion” standard (hereafter “RAS-approved identifiers”) set forth above. *Id.* at 10-11. However, because the alert list included all identifiers (foreign and domestic) that were of interest to counterterrorism analysts who were charged with tracking [REDACTED]

[REDACTED], most of the telephone identifiers compared against the incoming BR metadata were not RAS-approved.² Feb. 17, 2009 Memorandum at 10-11. Thus, since the earliest days of the FISC-authorized collection of call-detail records by the NSA, the

²As an example, the government reports that as of January 15, 2009, only 1,935 of the 17,835 identifiers on the alert list were RAS-approved. Feb.17, 2009 Memorandum at 11.

~~TOP SECRET//COMINT//NOFORN//MR~~

~~TOP SECRET//COMINT//NOFORN//MR~~

NSA has on a daily basis, accessed the BR metadata for purposes of comparing thousands of non-RAS approved telephone identifiers on its alert list against the BR metadata in order to identify any matches. Such access was prohibited by the governing minimization procedures under each of the relevant Court orders, as the government concedes in its submission. Feb. 17, 2009 Memorandum at 16.

The government's submission suggests that its non-compliance with the Court's orders resulted from a belief by some personnel within the NSA that some of the Court's restrictions on access to the BR metadata applied only to "archived data," *i.e.*, data residing within certain databases at the NSA. Feb. 17, 2009 Memorandum, Tab 1, Declaration of Lieutenant General Keith B. Alexander, United States Army, Director of the NSA ("Feb. 17, 2009 Alexander Declaration") at 10-11. That interpretation of the Court's Orders strains credulity. It is difficult to imagine why the Court would intend the applicability of the RAS requirement - a critical component of the procedures proposed by the government and adopted by the Court - to turn on whether or not the data being accessed has been "archived" by the NSA in a particular database at the time of the access. Indeed, to the extent that the NSA makes the decision about where to store incoming BR metadata and when the archiving occurs, such an illogical interpretation of the Court's Orders renders compliance with the RAS requirement merely optional.

The NSA also suggests that the NSA OGC's approval of procedures allowing the use of non-RAS-approved identifiers on the alert list to query BR metadata not yet in the NSA's "archive" was not surprising, since the procedures were similar to those used in connection with

~~TOP SECRET//COMINT//NOFORN//MR~~

~~TOP SECRET//COMINT//NOFORN//MR~~

other NSA SIGINT collection activities. Feb 17, 2009 Alexander Declaration at 11, n.6. If this is the case, then the root of the non-compliance is not a terminological misunderstanding, but the NSA's decision to treat the accessing of all call detail records produced by [REDACTED] no differently than other collections under separate NSA authorities, to which the Court-approved minimization procedures do not apply.

B. Misrepresentations to the Court

The government has compounded its non-compliance with the Court's orders by repeatedly submitting inaccurate descriptions of the alert list process to the FISC. Due to the volume of U.S. person data being collected pursuant to the Court's orders, the FISC's orders have all required that any renewal application include a report on the implementation of the Court's prior orders, including a description of the manner in which the NSA applied the minimization procedures set forth therein. See, e.g., BR 08-13, Primary Order at 12.

In its report to the FISC accompanying its first renewal application that was filed on August 18, 2006, the government described the alert list process as follows:

NSA has compiled through its continuous counter-terrorism analysis, a list of telephone numbers that constitutes an "alert list" of telephone numbers used by members of [REDACTED]. This alert list serves as a body of telephone numbers employed to query the data....

[...] Each of the foreign telephone numbers that comes to the attention of the NSA as possibly related to [REDACTED] is evaluated to determine whether the information about it provided to NSA satisfies the reasonable articulable suspicion standard. If so, the foreign telephone number is placed on the alert list; if not, it is not placed on the alert list.

The process set out above applies also to newly discovered domestic

~~TOP SECRET//COMINT//NOFORN//MR~~

~~TOP SECRET//COMINT//NOFORN//MR~~

telephone numbers considered for addition to the alert list, with the additional requirement that NSA's Office of General Counsel reviews these numbers and affirms that the telephone number is not the focus of the analysis based solely on activities that are protected by the First Amendment....

....

As of the last day of the reporting period addressed herein, NSA had included a total of 3980 telephone numbers on the alert list, which includes foreign numbers and domestic numbers, after concluding that each of the foreign telephone numbers satisfied the [RAS standard], and each of the domestic telephone numbers was either a FISC approved number or in direct contact with a foreign seed that met those criteria.^{3]}

To summarize the alert system: every day new contacts are automatically revealed with the 3980 telephone numbers contained on the alert list described above, which themselves are present on the alert list either because they satisfied the reasonable articulable suspicion standard, or because they are domestic numbers that were either a FISC approved number or in direct contact with a number that did so. These automated queries identify any new telephone contacts between the numbers on the alert list and any other number, except that domestic numbers do not alert on domestic-to-domestic contacts.

NSA Report to the Foreign Intelligence Surveillance Court, Docket no. BR 06-05, filed Aug. 18, 2006 at 12-15 (emphasis added). This description was included in similar form in all subsequent reports to the Court, including the report submitted to this Court on December 11, 2008. Feb. 17, 2009 Memorandum at 13.

The NSA attributes these material misrepresentations to the failure of those familiar with

³The report further explained that identifiers within the second category of domestic numbers were not used as "seeds." NSA Report to the Foreign Intelligence Surveillance Court, Docket no. BR 06-05, filed Aug. 18, 2006 at 14. Moreover, rather than conducting daily queries of the RAS-approved foreign telephone identifier that originally contacted the domestic number, the domestic numbers were included in the alert list as "merely a quicker and more efficient way of achieving the same result..." *Id.* at 14 n.6. In November 2006, the NSA reported that it ceased this activity on August 18, 2006. Feb. 17, 2009 Alexander Declaration at 7 n.1.

~~TOP SECRET//COMINT//NOFORN//MR~~

~~TOP SECRET//COMINT//NOFORN//MR~~

the program to correct inaccuracies in a draft of the report prepared in August 2006 by a managing attorney in the NSA's Office of General Counsel, despite his request that recipients of the draft "make sure everything I have said (sic) is absolutely true."⁴ Feb. 17, 2009 Alexander Declaration at 16-17; see also id. at Exhibit D. Further, the NSA reports:

it appears there was never a complete understanding among the key personnel who reviewed the report for the SIGINT Directorate and the Office of General Counsel regarding what each individual meant by the terminology used in the report. Once this initial misunderstanding occurred, the alert list description was never corrected since neither the SIGINT Directorate nor the Office of General Counsel realized there was a misunderstanding. As a result, NSA never revisited the description of the alert list that was included in the original report to the Court.

Feb. 17, 2009 Alexander Declaration at 18. Finally, the NSA reports that "from a technical standpoint, there was no single person who had a complete technical understanding of the BR FISA system architecture. This probably also contributed to the inaccurate description of the alert list that NSA included in its BR FISA reports to the Court." Id. at 19.

Regardless of what factors contributed to making these misrepresentations, the Court finds that the government's failure to ensure that responsible officials adequately understood the NSA's alert list process, and to accurately report its implementation to the Court, has prevented,

⁴The Court notes that at a hearing held on August 18, 2006, concerning the government's first renewal application (BR 06-08), the NSA's affiant testified as follows:

THE COURT: All right. Now additionally, you have cause to be -- well at least I received it yesterday -- the first report following the May 24 order, which is a 90-day report, _____ and some 18 pages and I've reviewed that and you affirm that that's the best report or true and accurate to the best of your knowledge and belief.

_____ I do, sir.

Transcript of Proceedings before the Hon. Malcolm J. Howard, U.S. FISC Judge, Docket No. BR 06-08, Aug. 18, 2006, at 12.

~~TOP SECRET//COMINT//NOFORN//MR~~

~~TOP SECRET//COMINT//NOFORN//MR~~

for more than two years, both the government and the FISC from taking steps to remedy daily violations of the minimization procedures set forth in FISC orders and designed to protect call detail records pertaining to telephone communications of U.S. persons located within the United States who are not the subject of any FBI investigation and whose call detail information could not otherwise have been legally captured in bulk.

C. Other Non-Compliance Matters

Unfortunately, the universe of compliance matters that have arisen under the Court's Orders for this business records collection extends beyond the events described above. On October 17, 2008, the government reported to the FISC that, after the FISC authorized the NSA to increase the number of analysts authorized to access the BR metadata to 85, the NSA trained those newly authorized analysts on Court-ordered procedures. Sixty-Day Report for Filing in Docket Number BR 08-08, filed Oct. 17, 2008 at 7. Despite this training, however, the NSA subsequently determined that 31 NSA analysts had queried the BR metadata during a five day period in April 2008 "without being aware they were doing so." *Id.* (emphasis added). As a result, the NSA analysts used 2,373 foreign telephone identifiers to query the BR metadata without first determining that the reasonable articulable suspicion standard had been satisfied. *Id.*

Upon discovering this problem, the NSA undertook a number of remedial measures, including suspending the 31 analysts' access pending additional training, and modifying the NSA's tool for accessing the data so that analysts were required specifically to enable access to

~~TOP SECRET//COMINT//NOFORN//MR~~

~~TOP SECRET//COMINT//NOFORN//MR~~

the BR metadata and acknowledge such access. Id. at 8. Despite taking these corrective steps, on December 11, 2008, the government informed the FISC that one analyst had failed to install the modified access tool and, as a result, inadvertently queried the data using five identifiers for which NSA had not determined that the reasonable articulable suspicion standard was satisfied. Preliminary Notice of Compliance Incident, Docket no. BR 08-08, filed Dec. 11, 2008 at 2; see also Notice of Compliance Incident Involving Docket Number BR 08-08, filed Jan. 22, 2009. Then, on January 26, 2009, the government informed the Court that, from approximately December 10, 2008, to January 23, 2009, two NSA analysts had used 280 foreign telephone identifiers to query the BR metadata without determining that the Court's reasonable articulable suspicion standard had been satisfied. Notice of Compliance Incident, Docket No. BR 08-13, filed January 26, 2009 at 2. It appears that these queries were conducted despite full implementation of the above-referenced software modifications to the BR metadata access tool, as well as the NSA's additional training of its analysts.⁵ And, as noted below with regard to the NSA's routine use of the [redacted] tool from May 2006 until February 18, 2009, the NSA continues to uncover examples of systemic noncompliance.

In summary, since January 15, 2009, it has finally come to light that the FISC's authorizations of this vast collection program have been premised on a flawed depiction of how

⁵On October 17, 2008, the government reported that all but four analysts who no longer required access to the BR metadata had completed the additional training and were provided access to the data. Sixty-Day Report for Filing in Docket Number BR 08-08, filed Oct. 17, 2008 at 8 n.6.

~~TOP SECRET//COMINT//NOFORN//MR~~

~~TOP SECRET//COMINT//NOFORN//MR~~

the NSA uses BR metadata. This 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. The minimization procedures proposed by the government in each successive application and approved and adopted as binding by the orders of the FISC have been so frequently and systemically violated that it can fairly be said that this critical element of the overall BR regime has never functioned effectively.

D. Reassessment of BR Metadata Authorization

In light of the foregoing, the Court returns to fundamental principles underlying its authorizations. In order to compel the production of tangible things to the government, the Court must find that there are reasonable grounds to believe that the tangible things sought are relevant to an authorized investigation (other than a threat assessment) to obtain foreign intelligence information not concerning a U.S. person or to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a U.S. person is not conducted solely on the basis of activities protected by the First Amendment. 50 U.S.C. § 1861.

The government's applications have all acknowledged that, of the _____ of call detail records NSA receives per day (currently over _____ per day), the vast majority of individual records that are being sought pertain neither to _____

_____. See, e.g., BR 08-13, Application at 19-20. In other words,

~~TOP SECRET//COMINT//NOFORN//MR~~

~~TOP SECRET//COMINT//NOFORN//MR~~

nearly all of the call detail records collected pertain to communications of non-U.S. persons who are not the subject of an FBI investigation to obtain foreign intelligence information, are communications of U.S. persons who are not the subject of an FBI investigation to protect against international terrorism or clandestine intelligence activities, and are data that otherwise could not be legally captured in bulk by the government. Ordinarily, this alone would provide sufficient grounds for a FISC judge to deny the application.

Nevertheless, the FISC has authorized the bulk collection of call detail records in this case based upon: (1) the government's explanation, under oath, of how the collection of and access to such data are necessary to analytical methods that are vital to the national security of the United States; and (2) minimization procedures that carefully restrict access to the BR metadata and include specific oversight requirements. Given the Executive Branch's responsibility for and expertise in determining how best to protect our national security, and in light of the scale of this bulk collection program, the Court must rely heavily on the government to monitor this program to ensure that it continues to be justified, in the view of those responsible for our national security, and that it is being implemented in a manner that protects the privacy interests of U.S. persons as required by applicable minimization procedures. To approve such a program, the Court must have every confidence that the government is doing its utmost to ensure that those responsible for implementation fully comply with the Court's orders. The Court no longer has such confidence.

~~TOP SECRET//COMINT//NOFORN//MR~~

~~TOP SECRET//COMINT//NOFORN//MR~~

With regard to the value of the BR metadata program, the government points to the 275 reports that the NSA has provided to the FBI identifying 2,549 telephone identifiers associated with the targets. Feb. 17, 2009 Alexander Declaration at 42. The government's submission also cites three examples in which the FBI opened three new preliminary investigations of persons in the U.S. based on tips from the BR metadata program. *Id.*, FBI Feedback on Report, Exhibit J. However, the mere commencement of a preliminary investigation, by itself, does not seem particularly significant. Of course, if such an investigation led to the identification of a previously unknown terrorist operative in the United States, the Court appreciates that it would be of immense value to the government. In any event, this program has been ongoing for nearly three years. The time has come for the government to describe to the Court how, based on the information collected and analyzed during that time, the value of the program to the nation's security justifies the continued collection and retention of massive quantities of U.S. person information.

Turning to the government's implementation of the Court-ordered minimization procedures and oversight regime, the Court takes note of the remedial measures being undertaken by the government as described in its recent filings. In particular, the Court welcomes the Director of the NSA's decision to order "end-to-end system engineering and process reviews (technical and operational) of NSA's handling" of BR metadata. Feb. 17, 2009 Alexander Declaration at 21. However, the Court is very disturbed to learn that this ongoing exercise has identified additional violations of the Court's orders, including the routine accessing of BR

~~TOP SECRET//COMINT//NOFORN//MR~~

~~TOP SECRET//COMINT//NOFORN//MR~~

metadata from May 2006 to February 18, 2009, through another NSA analytical tool known as _____ using telephone identifiers that had not been determined to meet the reasonable articulable suspicion standard. BR 08-13, Notice of Compliance Incident, filed Feb. 26, 2009 (“Feb. 26, 2009 Notice”).

In its last submission, the government describes technical measures implemented on February 20, 2009, designed to prevent any recurrences of the particular forms of non-compliance uncovered to date. This “technical safeguard” is intended to prevent “any automated process or subroutine,” such as _____ “from accessing the BR FISA data,” and to prevent “analysts from performing manual chaining⁶] on numbers that have not been marked as RAS approved.” See Supplemental Declaration of Lieutenant General Keith B. Alexander, United States Army, Director of NSA, filed Feb. 26, 2009 (“Feb. 26, 2009 Alexander Declaration”) at 7 & n.2. On the strength of these measures, the government submits that “the Court need not take any further remedial action.” Feb. 26, 2009 Notice at 6. After considering these measures in the context of the historical record of non-compliance and in view of the Court’s authority and responsibility to “determine [and] enforce compliance” with Court orders and Court-approved procedures, 50 U.S.C. § 1803(i), the Court has concluded that further action is, in fact, necessary.

The record before the Court strongly suggests that, from the inception of this FISA BR

⁶ In context, “chaining” appears to refer to the form of querying the BR metadata known as “contact chaining.” See _____ Declaration at 6.

~~TOP SECRET//COMINT//NOFORN//MR~~

~~TOP SECRET//COMINT//NOFORN//MR~~

program, the NSA's data accessing technologies and practices were never adequately designed to comply with the governing minimization procedures. From inception, the NSA employed two separate automated processes – the daily alert list and the [] tool – that routinely involved queries based on telephone identifiers that were not RAS-approved. See supra pp. 4-6, 13-14. As for manual queries, the minimization procedures required analysts to use RAS-approved identifiers whenever they accessed BR metadata, yet thousands of violations resulted from the use of identifiers that had not been RAS-approved by analysts who were not even aware that they were accessing BR metadata. See supra pp. 9-10.

Moreover, it appears that the NSA – or at least those persons within the NSA with knowledge of the governing minimization procedures – are still in the process of determining how the NSA's own systems and personnel interact with the BR metadata. Under these circumstances, no one inside or outside of the NSA can represent with adequate certainty whether the NSA is complying with those procedures. In fact, the government acknowledges that, as of August 2006, "there was no single person who had a complete understanding of the BR FISA system architecture." Feb. 17, 2009 Alexander Declaration at 19. This situation evidently had not been remedied as of February 18, 2009, when "NSA personnel determined," only as a result of the "end-to-end review of NSA's technical infrastructure" ordered by the Director of the NSA on January 15, 2009, that the [] tool accessed the BR metadata on the basis of telephone identifiers that had not been RAS-approved. Feb. 26, 2009 Alexander Declaration at 2-3.

~~TOP SECRET//COMINT//NOFORN//MR~~

~~TOP SECRET//COMINT//NOFORN//MR~~

This end-to-end review has not been completed. Id. at 10. Nonetheless, the government submits that the technical safeguards implemented on February 20, 2009 “should prevent recurrences” of the identified forms of non-compliance, id. at 9 (emphasis added), and “expect[s] that any further problems NSA personnel may identify with the infrastructure will be historical,” rather than current, id. at 10 (emphasis added). However, until this end-to-end review has been completed, the Court sees little reason to believe that the most recent discovery of a systemic, ongoing violation – on February 18, 2009 – will be the last. Nor does the Court share the government’s optimism that technical safeguards implemented to respond to one set of problems will fortuitously be effective against additional problems identified in the future.

Moreover, even with regard to the particular forms of non-compliance that have been identified, there is reason to question whether the newly implemented safeguards will be effective. For example, as discussed above, the NSA reported on October 17, 2008, that it had deployed software modifications that would require analysts to specifically enable access to BR metadata when performing manual queries, but these modifications did not prevent hundreds of additional violations by analysts who inadvertently accessed BR metadata through queries using telephone identifiers that had not been RAS-approved. See supra pp. 9-10; Feb. 26, 2009 Alexander Declaration at 4. The Court additionally notes that, in a matter before another judge of the FISC, _____

_____ the mere existence of software solutions was not sufficient to ensure their efficacy:

~~TOP SECRET//COMINT//NOFORN//MR~~

~~TOP SECRET//COMINT//NOFORN//MR~~

- “NSA’s representations to the Court in the August 27, 2008, hearing did not explicitly account for the possibility that system configuration errors (such as those discussed in the government’s response to question 10 below) might render NSA’s overcollection filters ineffective, which was the root cause for some of the non-compliance incidents.”
Government’s Response to the Court’s Order of January 16, 2009, answer no. 8 at 13.
- “Troubleshooting has since revealed that a software patch that might have prevented the [compliance incident] was not present on the recently deployed selection system.” Id., answer no. 10 at 14.
- “NSA further determined [in January 2009] that the overcollection filter had not been functioning since this site was activated on July 30, 2008.” Id.

In light of what appear to be systemic problems, this Court cannot accept the mere introduction of technological remedies as a demonstration that a problem is solved. More is required. Thus, notwithstanding the remedial measures undertaken by the government, the Court believes that more is needed to protect the privacy of U.S. person information acquired and retained pursuant to the FISC orders issued in this matter. However, given the government’s repeated representations that the collection of the BR metadata is vital to national security, and in light of the Court’s prior determinations that, if the program is conducted in compliance with appropriate minimization procedures, such collection conforms with 50 U.S.C. §1861, the Court concludes it would not be prudent to order that the government’s acquisition of the BR metadata cease at this

~~TOP SECRET//COMINT//NOFORN//MR~~

~~TOP SECRET//COMINT//NOFORN//MR~~

time. However, except as authorized below, the Court will not permit the government to access the data collected until such time as the government is able to restore the Court's confidence that the government can and will comply with previously approved procedures for accessing such data.

Accordingly, it is HEREBY ORDERED:

1. The NSA may continue to acquire all call detail records of "telephony metadata" created by [REDACTED] in accordance with the orders entered in the above-captioned docket on December 12, 2008;

2. The government is hereby prohibited from accessing BR metadata acquired pursuant to FISC orders in the above-captioned docket and its predecessors for any purpose except as described herein. The data may be accessed for the purpose of ensuring data integrity and compliance with the Court's orders. Except as provided in paragraph 3, access to the BR metadata shall be limited to the team of NSA data integrity analysts described in footnote 5 of the [REDACTED] Declaration, and individuals directly involved in developing and testing any technological measures designed to enable the NSA to comply with previously approved procedures for accessing such data;

3. The government may request through a motion that the Court authorize querying of the BR metadata for purposes of obtaining foreign intelligence on a case-by-case basis. However, if the government determines that immediate access is necessary to protect against an imminent threat to human life, the government may access the BR metadata for such purpose. In

~~TOP SECRET//COMINT//NOFORN//MR~~

~~TOP SECRET//COMINT//NOFORN//MR~~

each such case falling under this latter category, the government shall notify the Court of the access, in writing, no later than 5:00 p.m., Eastern Time on the next business day after such access. Any submission to the Court under this paragraph shall, at a minimum, specify the telephone identifier for which access is sought or was granted, provide the factual basis for the NSA's determination that the reasonable articulable suspicion standard has been met with regard to that identifier, and, if the access has already taken place, a statement of the immediate threat necessitating such access;

4. Upon completion of the government's end-to-end system engineering and process reviews, the government shall file a report with the Court, that shall, at a minimum, include:

a. an affidavit by the Director of the FBI, and affidavits by any other official responsible for national security that the government deems appropriate, describing the value of the BR metadata to the national security of the United States and certifying that the tangible things sought are relevant to an authorized investigation (other than a threat assessment) to obtain foreign intelligence information not concerning a U.S. person or to protect against international terrorism or clandestine intelligence activities, and that such investigation of a U.S. person is not conducted solely on the basis of activities protected by the First Amendment;

b. a description of the results of the NSA's end-to-end system engineering and process reviews, including any additional instances of non-compliance identified therefrom;

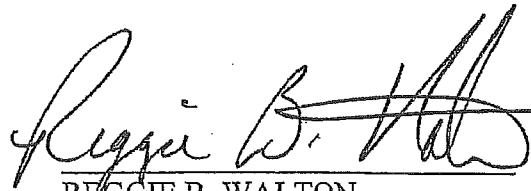
~~TOP SECRET//COMINT//NOFORN//MR~~

~~TOP SECRET//COMINT//NOFORN//MR~~

c. a full discussion of the steps taken to remedy any additional non-compliance as well as the incidents described herein, and an affidavit attesting that any technological remedies have been tested and demonstrated to be successful; and

d. the minimization and oversight procedures the government proposes to employ should the Court decide to authorize the government's resumption of regular access to the BR metadata.

IT IS SO ORDERED, this 2nd day of March, 2009.



REGGIE B. WALTON

Judge, United States Foreign Intelligence
Surveillance Court

~~TOP SECRET//COMINT//NOFORN//MR~~

Exhibit 5



Too tempting? NSA watchdog details how officials spied on love interests

By Jake Gibson

Published September 27, 2013 | FoxNews.com

The world learned in early June about the National Security Agency's stunning capability to spy on just about anyone it wants to. Now we're finding out that power was just too tempting for some of its own employees -- with the agency acknowledging that workers used NSA tools to spy on love interests.

In a letter to Sen. Chuck Grassley, R-Iowa, NSA Inspector General George Ellard admitted that since 2003, there have been "12 substantiated instances of intentional misuse" of "surveillance authorities," and "SIGINT," or signals intelligence.

Just about all of these cases involve an NSA employee spying on a girlfriend, boyfriend or some kind of love interest, or "loveint." Media reports had earlier claimed NSA workers were engaged in this kind of activity. The letter to Grassley gave specific details for the first time.

According to the letter, just prior to a polygraph examination in 2011 one NSA employee admitted that he queried information on his girlfriend's phone "out of curiosity." However, that "subject retired in 2012 before disciplinary action had been taken."

Another employee went much further, tracking nine different telephone numbers for "female foreign nationals, without a valid foreign intelligence purpose" between 1998 and 2003 -- and listening to the phone conversations. The activity was uncovered after a female foreign national employed by the U.S. government, who was having sexual relations with the offending employee, told a colleague she thought her phone was being tapped.

In another instance, a female NSA employee admitted in 2004 to tapping a telephone number she found in her husband's cell phone "because she suspected that her husband had been unfaithful." In this case the NSA employee resigned before any disciplinary action.

The IG wrote that there are two additional open investigations into similar misuse of intelligence capabilities and yet another allegation for possible investigation.

Grassley, the top Republican on the Senate Judiciary Committee, said in a statement that the NSA should have a zero-tolerance policy toward abuse.

"I appreciate the transparency that the Inspector General has provided to the American people. We shouldn't tolerate even one instance of misuse of this program," he said. "Robust oversight of the program must be completed to ensure that both national security and the Constitution are protected."



URL

<http://www.foxnews.com/politics/2013/09/27/too-tempting-nsa-details-how-officials-spied-on-love-interests/>

[Home](#) | [Video](#) | [Politics](#) | [U.S.](#) | [Opinion](#) | [Entertainment](#) | [Tech](#) | [Science](#) | [Health](#) | [Travel](#) | [Lifestyle](#) | [World](#) | [Sports](#) | [Weather](#)

[Privacy](#) | [Terms](#)

This material may not be published, broadcast, rewritten, or redistributed. © 2014 FOX News Network, LLC. All rights reserved. All market data delayed 20 minutes.

Exhibit 6

National Security

NSA broke privacy rules thousands of times per year, audit finds



By **Barton Gellman** August 15, 2013

Follow @bartongellman

The National Security Agency has broken privacy rules or overstepped its legal authority thousands of times each year since Congress granted the agency broad new powers in 2008, according to [an internal audit](#) and other top-secret documents.

Most of the infractions involve unauthorized surveillance of Americans or foreign intelligence targets in the United States, both of which are restricted by statute and executive order. They range from significant violations of law to typographical errors that resulted in unintended interception of U.S. e-mails and telephone calls.

The Most Popular All Over

SLATE

Help! My Husband's Spent Our Entire Marriage Writing a...

THE WASHINGTON POST

Ex-SEAL Robert O'Neill reveals himself as shooter who killed...

ST. LOUIS POST-DISPATCH

Coalition wants advance notice, de-militarized police response...

Our Online Games

Play right from this page

Spider Solitaire

The documents, provided earlier this summer to The Washington Post by former NSA contractor Edward Snowden, include a level of detail and analysis that is not routinely shared with Congress or the special court that oversees surveillance. In [one of the documents](#), agency personnel are instructed to remove details and substitute more generic language in reports to the Justice Department and the Office of the Director of National Intelligence.

In one instance, the NSA decided that it need not report the unintended surveillance of Americans. A notable example in 2008 was the interception of a “large number” of calls placed from Washington when a programming error confused the U.S. area code 202 for 20, the international dialing code for Egypt, according to a “quality assurance” review that was not distributed to the NSA’s oversight staff.

In another case, the Foreign Intelligence Surveillance Court, which has authority over some NSA operations, did not learn about a new collection method until it had been in operation for many months. The court ruled it unconstitutional.

Read the documents

NSA report on privacy violations

Read the full report with key sections highlighted

Genre(s): Card

Spider Solitaire is known as the king of all solitaire games!

52 card pickup

Genre(s): Card

Pick up cards as fast as you can!

Tri-Peaks Solitaire

Genre(s): Card

Reveal cards as you clear your way to the top!

Carniball

Genre(s): Arcade

This amusement park classic will bring back some joyous memories

FISA court finds illegal surveillance

The only known details of a 2011 ruling that found the NSA was using illegal methods to collect and handle the communications of American citizens.

What's a 'violation'?

View a slide used in a training course for NSA intelligence collectors and analysts.

What to say (and what not to say)

How NSA analysts explain their targeting decisions without giving "extraneous information" to overseers.

[\[FISA judge: Ability to police U.S. spying program is limited\]](#)

The Obama administration has provided almost no public information about the NSA's compliance record. In June, after promising to explain the NSA's record in "as transparent a way as we possibly can," Deputy Attorney General James Cole described extensive safeguards and oversight that keep the agency in check. "Every now and then, there may be a mistake," Cole said in congressional testimony.

2012, counted 2,776 incidents in the preceding 12 months of unauthorized collection, storage, access to or distribution of legally protected communications. Most were unintended. Many involved failures of due diligence or violations of standard operating procedure. The most serious incidents included a violation of a court order and unauthorized use of data about more than 3,000 Americans and green-card holders.

In a [statement in response to questions for this article](#), the NSA said it attempts to identify problems “at the earliest possible moment, implement mitigation measures wherever possible, and drive the numbers down.” The government was made aware of The Post’s intention to publish the documents that accompany this article online.

“We’re a human-run agency operating in a complex environment with a number of different regulatory regimes, so at times we find ourselves on the wrong side of the line,” a senior NSA official said in an interview, speaking with White House permission on the condition of anonymity.

“You can look at it as a percentage of our total activity that occurs each day,” he said. “You look at a number in absolute terms that looks big, and when you look at it in relative terms, it looks a little

There is no reliable way to calculate from the number of recorded compliance issues how many Americans have had their communications improperly collected, stored or distributed by the NSA.

The causes and severity of NSA infractions vary widely. One in 10 incidents is attributed to a typographical error in which an analyst enters an incorrect query and retrieves data about U.S phone calls or e-mails.

But the more serious lapses include unauthorized access to intercepted communications, the distribution of protected content and the use of automated systems without built-in safeguards to prevent unlawful surveillance.

The [May 2012 audit](#), intended for the agency's top leaders, counts only incidents at the NSA's Fort Meade headquarters and other facilities in the Washington area. Three government officials, speaking on the condition of anonymity to discuss classified matters, said the number would be substantially higher if it included other NSA operating units and regional collection centers.

Senate Intelligence Committee Chairman Dianne Feinstein (D-Calif.), who did not receive a copy of

the 2012 audit until The Post asked her staff about it.

said in a statement late Thursday that the committee “can and should do more to independently verify that NSA’s operations are appropriate, and its reports of compliance incidents are accurate.”

Despite the quadrupling of the NSA’s oversight staff after a series of significant violations in 2009, the rate of infractions increased throughout 2011 and early 2012. An NSA spokesman declined to disclose whether the trend has continued since last year.

One major problem is largely unpreventable, the audit says, because current operations rely on technology that cannot quickly determine whether a foreign mobile phone has entered the United States.

In what appears to be one of the most serious violations, the NSA diverted large volumes of international data passing through fiber-optic cables in the United States into a repository where the material could be stored temporarily for processing and selection.

The operation to obtain what the agency called “multiple communications transactions” collected and commingled U.S. and foreign e-mails, according to an article in SSO News, a top-secret internal newsletter of the NSA’s Special Source Operations unit. NSA lawyers told the court that the agency

could not practicably filter out the communications of Americans.

In October 2011, months after the program got underway, the Foreign Intelligence Surveillance Court ruled that the collection effort was unconstitutional. The court said that the methods used were “deficient on statutory and constitutional grounds,” according to a top-secret summary of the opinion, and it ordered the NSA to comply with standard privacy protections or stop the program.

James R. Clapper Jr., the director of national intelligence, has acknowledged that the court found the NSA in breach of the Fourth Amendment, which prohibits unreasonable searches and seizures, but the Obama administration has fought a Freedom of Information lawsuit that seeks the opinion.

Generally, the NSA reveals nothing in public about its errors and infractions. The unclassified versions of the administration’s semiannual reports to Congress feature blacked-out pages under the headline “Statistical Data Relating to Compliance Incidents.”

Members of Congress may read the unredacted documents, but only in a special secure room, and they are not allowed to take notes. Fewer than 10 percent of lawmakers employ a staff member who

has the security clearance to read the reports and

provide advice about their meaning and significance.

The limited portions of the reports that can be read by the public acknowledge “a small number of compliance incidents.”

Under NSA auditing guidelines, the incident count does not usually disclose the number of Americans affected.

“What you really want to know, I would think, is how many innocent U.S. person communications are, one, collected at all, and two, subject to scrutiny,” said Julian Sanchez, a research scholar and close student of the NSA at the Cato Institute.

The documents provided by Snowden offer only glimpses of those questions. Some reports make clear that an unauthorized search produced no records. But a single “incident” in February 2012 involved the unlawful retention of 3,032 files that the surveillance court had ordered the NSA to destroy, according to the May 2012 audit. Each file contained an undisclosed number of telephone call records.

One of the documents sheds new light on a statement by NSA Director Keith B. Alexander last year that “we don’t hold data on U.S. citizens.”

the condition of anonymity, have defended

Alexander with assertions that the agency's internal definition of "data" does not cover "metadata" such as the trillions of American call records that the NSA is now known to have collected and stored since 2006. Those records include the telephone numbers of the parties and the times and durations of conversations, among other details, but not their content or the names of callers.

The NSA's authoritative definition of data includes those call records. "Signals Intelligence Management Directive 421," which is quoted in secret oversight and auditing guidelines, states that "raw SIGINT data ... includes, but is not limited to, unevaluated and/or unminimized transcripts, gists, facsimiles, telex, voice, and some forms of computer-generated data, such as call event records and other Digital Network Intelligence (DNI) metadata as well as DNI message text."

In the case of the collection effort that confused calls placed from Washington with those placed from Egypt, it is unclear what the NSA meant by a "large number" of intercepted calls. A spokesman declined to discuss the matter.

The NSA has different reporting requirements for each branch of government and each of its legal

authorities. The “202” collection was deemed irrelevant to any of them. “The issue pertained to Metadata ONLY so there were no defects to report,” according to the author of the secret memo from March 2013.

The large number of database query incidents, which involve previously collected communications, confirms long-standing suspicions that the NSA’s vast data banks — with code names such as MARINA, PINWALE and XKEYSCORE — house a considerable volume of information about Americans. Ordinarily the identities of people in the United States are masked, but intelligence “customers” may request unmasking, either one case at a time or in standing orders.

In dozens of cases, NSA personnel made careless use of the agency’s extraordinary powers, according to individual auditing reports. One team of analysts in Hawaii, for example, asked a system called DISHFIRE to find any communications that mentioned both the Swedish manufacturer Ericsson and “radio” or “radar” — a query that could just as easily have collected on people in the United States as on their Pakistani military target.

The NSA uses the term “incidental” when it sweeps up the records of an American while targeting a foreigner or a U.S. person who is believed to be

personnel say that kind of incident, pervasive under current practices, “does not constitute a . . . violation” and “does not have to be reported” to the NSA inspector general for inclusion in quarterly reports to Congress. Once added to its databases, absent other restrictions, the communications of Americans may be searched freely.

In one required tutorial, NSA collectors and analysts are taught to fill out oversight forms without giving “extraneous information” to “our FAA overseers.” FAA is a reference to the FISA Amendments Act of 2008, which granted broad new authorities to the NSA in exchange for regular audits from the Justice Department and the Office of the Director of National Intelligence and periodic reports to Congress and the surveillance court.

Using real-world examples, the “Target Analyst Rationale Instructions” explain how NSA employees should strip out details and substitute generic descriptions of the evidence and analysis behind their targeting choices.

“I realize you can read those words a certain way,” said the high-ranking NSA official who spoke with White House authority, but the instructions were not intended to withhold information from auditors. “Think of a book of individual recipes,” he said. Each

target “has a short, concise description,” but that is

USCA Case #14-5004

Document #1521428

Filed: 11/07/2014

Page 181 of 194

“not a substitute for the full recipe that follows,
which our overseers also have access to.”

Julie Tate and Carol D. Leonnig contributed to this
report.

Barton Gellman writes for the national staff. He has
contributed to three Pulitzer Prizes for The Washington Post,
most recently the 2014 Pulitzer Prize for Public Service.

August 16, 2013

N.S.A. Often Broke Rules on Privacy, Audit Shows

By CHARLIE SAVAGE

WASHINGTON — The [National Security Agency](#) violated privacy rules protecting the communications of Americans and others on domestic soil 2,776 times over a one-year period, according to an internal audit leaked by the former N.S.A. contractor Edward J. Snowden and made public on Thursday night.

The violations, according to the May 2012 audit, stemmed largely from operator and system errors like “inadequate or insufficient research” when selecting wiretap targets.

The largest number of episodes — 1,904 — appeared to be “roamers,” in which a foreigner whose cellphone was being wiretapped without a warrant came to the United States, where individual warrants are required. A spike in such problems in a single quarter, the report said, could be because of Chinese citizens visiting friends and family for the Chinese Lunar New Year holiday.

“Roamer incidents are largely unpreventable, even with good target awareness and traffic review, since target travel activities are often unannounced and not easily predicted,” the report says.

The report and several other documents leaked by Mr. Snowden [were published by The Washington Post](#). They shed new light on the intrusions into Americans’ privacy that N.S.A. surveillance can entail, and how the agency handles violations of its rules.

Mr. Snowden, who was recently granted temporary asylum in Russia, is believed to have given the documents to The Post months ago.

The Post, which did not publish every document its accompanying article relied upon, cited other problems as well. In one case in 2008 that was not reported to the Foreign Intelligence Surveillance Court or Congress, it said, the system collected metadata logs about a “large number” of calls dialed from Washington — something it was already doing through a program — because of a programming error mixing up the district’s area code, international dialing code of Egypt, 20.

Jameel Jaffer of the American Civil Liberties Union said that while some of th

OPEN

MORE IN U.
[Midterm Aren't /](#)
[Read More](#)

violations were more troubling than others, the sheer number of them was “jaw-dropping.”

In a statement, the N.S.A. said its surveillance activities “are continually audited and overseen internally and externally.”

“When N.S.A. makes a mistake in carrying out its foreign intelligence mission, the agency reports the issue internally and to federal overseers — and aggressively gets to the bottom of it,” the statement said.

Another newly disclosed document included instructions for how N.S.A. analysts should record their rationales for eavesdropping under the FISA Amendments Act, or F.A.A., which allows wiretapping without warrants on domestic networks if the target is a noncitizen abroad. The document said analysts should keep descriptions of why the people they are targeting merit wiretapping to “one short sentence” and avoid details like their names and supporting information.

“While we do want to provide our F.A.A. overseers with the information they need, we DO NOT want to give them any extraneous information,” it said.

A brief article in an internal N.S.A. newsletter offered hints about a known but little-understood episode in which the [Foreign Intelligence Surveillance Court](#) found in 2011 that the N.S.A. had violated the Fourth Amendment. The newsletter said the court issued an 80-page ruling on Oct. 3, 2011, finding that something the N.S.A. was collecting involving “Multiple Communications Transactions” on data flowing through fiber-optic networks on domestic soil was “deficient on statutory and constitutional grounds.”

In a statement, the N.S.A. said the problem related to “a very specific and highly technical aspect,” which it reported to the court and Congress “once the issue was identified and fully understood.” Privacy protections for Americans were strengthened, it said, and the court allowed the surveillance to continue.

This article has been revised to reflect the following correction:

Correction: August 16, 2013

An earlier version of this article inaccurately portrayed an incident in 2008 involving a mix-up of the area code of Washington, D.C., 202, and the international dialing code of Egypt, 20. While the Washington Post initially described this incident as involving the “interception” of calls placed from Washington, the Post later explained that it involved the collection of “metadata” logs about the calls. It is not the case that the N.S.A. recorded the contents of the calls.

Report: 2,776 privacy violations by NSA in 12 months

August 15, 2013 | Reuters

Recommend { 11 } Tweet { 0 }

481 { g+1 } { 3 }

WASHINGTON (Reuters) - The National Security Agency has broken privacy rules or overstepped its legal authority thousands of times each year since 2008, the Washington Post reported on Thursday, citing an internal audit and other top-secret documents.

Most of the infractions involved unauthorized surveillance of Americans or foreign intelligence targets in the United States, both of which are restricted by law and executive order, the paper said.

They ranged from significant violations of law to typographical errors that resulted in unintended interception of U.S. emails and telephone calls, it said.

The Post said the documents it obtained were part of a trove of materials provided to the paper by former NSA contractor Edward Snowden, who has been charged by the United States with espionage. He was granted asylum in Russia earlier this month.

The documents included a level of detail and analysis that is not routinely shared with Congress or the special court that oversees surveillance, the paper said. In one of the documents, agency personnel are instructed to remove details and substitute more generic language in reports to the Justice Department and the Office of the Director of National Intelligence.

In one instance, the NSA decided it need not report the unintended surveillance of Americans, the Post said. A notable example in 2008 was the interception of a "large number" of calls placed from Washington when a



(http://www.trbimg.com/img-520e71fb/turbine/sns-rt-us-usa-security-radomes-that-contain-radar-antennas-stand-at-an-operating-facility-snowden-nsa-20130815-...

The Post said the NSA audit, dated May 2012, counted 2,776 incidents in the preceding 12 months of unauthorized collection, storage, access to or distribution of legally protected communications.

The paper said most were unintended. Many involved failures of due diligence or violations of standard operating procedure. It said the most serious incidents included a violation of a court order and unauthorized use of data about more than 3,000 Americans and green-card holders.

In 2008, the FISA Amendments Act granted NSA broad new powers in exchange for regular audits from the Justice Department and the office of the Director of National Intelligence and periodic reports to Congress and the surveillance court, the Post said.

"We're a human-run agency operating in a complex environment with a number of different regulatory regimes, so at times we find ourselves on the wrong side of the line," a senior NSA official, speaking on the condition of anonymity, told the Post.

"You can look at it as a percentage of our total activity that occurs each day," he said. "You look at a number in absolute terms that looks big, and when you look at it in relative terms, it looks a little different."

In what the Post said appeared to be one of the most serious violations, the NSA diverted large volumes of international data passing through fiber-optic cables in the United States into a repository where the material could be stored temporarily for processing and selection.

The operation collected and commingled U.S. and foreign emails, the Post said, citing a top-secret internal NSA newsletter. NSA lawyers told the Foreign Intelligence Surveillance Court that the agency could not practicably filter out the communications of Americans.

In October 2011, months after the program got underway, the court ruled that the collection effort was unconstitutional.

Some members of the Senate Intelligence Committee, including Democrat Ron Wyden of Oregon, have been trying for some time to get the NSA to give some kind of accounting of how much data it collects "incidentally" on Americans through various electronic dragnets. The Obama administration has strongly resisted such disclosures.

(Writing by Eric Beech; Editing by David Brunnstrom)

Featured Articles



Michael Jordan marries longtime girlfriend (/2013-04-27/sports/sns-rt-bkn-bobcats-bulls-newssx5b6d3a1-20130427_1_juanita-vanoy-girlfriend-yvette-marriage-license)

Cause of ALS is found, Northwestern team says (/2011-08-22/news/ct-met-northwestern-als-breakthrough-20110822_1_als-patients-proteins-northwestern-research)

Body pulled from lake identified as 32-year-old Lake Forest woman (/2014-05-09/news/chi-body-pulled-from-lake-identified-as-32yearold-lake-forest-woman-20140509_1_boat-ramp-rebecca-long-lake-forest)

MORE:

Winter boot showdown (/2012-02-19/features/ct-sun-0219-warren-shopping-winter-boots-20120217_1_cold-feet-warmest-winter)

Pain relievers: What are the differences? (/2011-01-13/news/sc-health-0112-pain-reliever-differen20110113_1_alcohol-warning-chronic-pain-tylenol)

Illinois Woman On Death Row (/1991-02-21/news/9101170006_1_illinois-department-sentenced-illinois-prison-officials)

Rauner's many million-dollar homes (/2013-11-25/news/ct-met-bruce-rauner-homes-20131125_1_bruce-rauner-illinois-governor-mitt-romney)

10 reasons why you want the job (/2013-09-29/jobs/sns-201301161600--tms--careersntp--h-a20130123-20130123_1_job-interviewer-10-reasons)

U.s. Jury Convicts Cocaine Kingpin (/1999-05-25/news/9905250177_1_drug-count-money-laundering-co-defendant)

Related Articles

NSA broke privacy rules thousands of times per year -report (/2013-08-15/news/sns-rt-usa-securitysnowden-nsa-20130815_1_washington-post-senior-nsa-official-u-s-national-security-agency)

August 15, 2013

Obama defends surveillance effort as 'trade-off' for... (/2013-06-07/news/sns-rt-usa-security-recordsbre956ova-20130607_1_government-surveillance-president-barack-obama-privacy)

June 7, 2013

Editorial: When the NSA gets out of line (/2013-08-18/opinion/ct-edit-nsa-20130818_1_nsa-washington-post-domestic-phone-records)

August 18, 2013

Microsoft helped NSA, FBI access user info -Guardian (/2013-07-11/news/sns-rt-usa-cybersecuritymicrosoft-20130711_1_nsa-prism-program-national-security-agency)

July 11, 2013

Obama says he will propose NSA reforms (/2013-12-05/news/sns-rt-us-usa-security-nsa-20131127_1_nsa-programs-president-barack-obama-national-security-agency)

December 5, 2013

Find More Stories About

National Security Agency (/keyword/national-security-agency) Washington Post (/keyword/washington-post) National Intelligence (/keyword/national-intelligence)

Terms of Service

(<http://www.chicagotribune.com/tos/>)

Privacy Policy

(<http://www.chicagotribune.com/privacy/>)

Index by Date

(/2013/aug/15)

Index by Keyword

Connect (/keywords)

Like us on Facebook

www.chicagotribune.com

(<https://www.facebook.com/chicagotribune>)

(<http://www.chicagotribune.com>)

Follow us on Twitter

(<http://twitter.com/#!/chicagotribune>)

Chicago Tribune

THE AMERICAN PROSPECT

The NSA Can't Be Trusted

SCOTT LEMIEUX AUGUST 19, 2013

If 2,776 violations can occur when NSA agents are trying to follow the law in good faith, consider the dangers posed by personnel who aren't acting in good faith.



flickr/Alex Ellison

n August 9, President Obama **gave** a news conference at which he defended his

O administration's record on surveillance while proposing some modest reforms. Predictably, it got **mixed reviews** from observers concerned about civil liberties. Less than a week later, *The Washington Post* published **an important story** about the National Security Agency (NSA) that makes it clear more reforms are necessary—and undermine Obama's defense of his record.

The key finding of the story, by Scott Wilson and Zachary Goldfarb: An **internal audit** found 2,776 "incidents" in which NSA surveillance breached rules between April 2011 and March 2012. Even worse, the rates of illegal "incidents" have been increasing. As the *Post's* Timothy Lee **says**, "We now know that President Obama's assurances that the NSA wasn't 'actually abusing' its surveillance programs are untrue." The only question is whether Obama deliberately misled the public, or whether he was unaware of these violations. Neither possibility is very encouraging.

There are two possible arguments about why these violations are not quite as bad as the raw numbers make them sound, one which has merit and one which doesn't. The fair counterpoint is that a majority of these violations were inadvertent, based on the inability of the software to detect when foreign cellphones were in fact located in the United States. (The warrantless monitoring of calls made solely on American soil is generally illegal; the Foreign Intelligence Surveillance Act (FISA) covers only communications with at least one foreign party.) Roughly 10 percent of the violations were the result of clerical errors that caused the wrong numbers to be searched. These violations were inadvertent, but that doesn't make them trivial—it's a failure that raises important questions about the ability of statutory restrictions to limit warrantless searches. However, it is true that a majority of the breaches do not seem to have been the result of willful legal violations of the law.

The second line of defense, however, is less persuasive. The NSA argues in the *Post* story that the violations need to be viewed in the context of the total number of searches conducted by the NSA:

“You can look at it as a percentage of our total activity that occurs each day,” he said. “You look at a number in absolute terms that looks big, and when you look at it in relative terms, it looks a little different.”

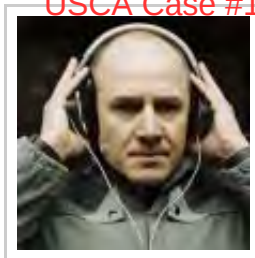
Viewing the violations in relative terms is relevant if we're evaluating the good faith of the agents within the NSA. In broader civil liberties terms, however, to focus on relative as opposed to absolute numbers is wrong. Precisely the problem with moving away from the typical requirement that searches and seizures require individualized suspicion is that the sheer scope of the NSA's searches increases the chances for violations of civil liberties. That the large number of violations occurred in the context of a huge number of searches is beside the point. The more searches, the greater the chances civil liberties violations will occur. Indeed, in this sense the fact that most of the errors seem to have been inadvertent is even more disturbing—if this number of violations can occur when agents are trying to follow the law in good faith, consider the dangers posed by NSA personnel who aren't acting in good faith.

Not all of these violations were minor, either. The NSA continued to use a broad search method that could not reliably distinguish between domestic and foreign communications for months before it was ruled unconstitutional by the FISA court. The **optimistic** way of looking at this story is to note that the system ultimately worked—normally **a near-rubber stamp**, the court properly exercised its oversight powers.

There's some truth to this, but this violation still raises some serious questions. It seems likely that the FISA court—which thanks to the unwise decision by Congress to confer the **unilateral power** to select FISA judges to the Chief Justice of the Supreme Court is dominated by conservative Republicans—is permitting the NSA to use techniques of questionable legality. The audit makes clear that the NSA is determined to push the legal envelope, and it's hard to view the FISA court as a reliable check on potential abuses. Indeed, the chief judge of the FISA court **has said** that his tribunal "does not have the capacity to investigate issues of noncompliance."

The leaked audit makes President Obama's reassurances about the NSA's surveillance regime ring hollower than ever. Above all, it **compellingly shows** the need for greater congressional oversight. It's never easy to be optimistic about Congress stepping up, but this important story will hopefully be a nudge in the right direction.

You may also like:



How All Three
Branches
Conspired to
Threaten Your
Privacy

One Small Step
for the Fourth
Amendment

Yet Another NSA
Violation

The Verizon Data
Order and Why It
Matters

Federal Board
Finds NSA
Program Illegal
and Unjustified

© 2014 by The American Prospect

← Back to Original Article

National Security Agency broke privacy rules, documents show

The leaked papers spur new calls to restrict surveillance of Americans and threaten to further erode trust in the spy agency.

August 16, 2013 | By Ken Dilanian

WASHINGTON — Leaked documents showing the National Security Agency overstepped its legal authority thousands of times since 2011 have spurred new calls to restrict surveillance on Americans and threatened to further erode trust in the powerful spy agency.

In an attempt to contain the damage Friday, intelligence officials rushed to brief congressional staffers and the White House issued a statement of support for the NSA, which critics say has violated Americans' privacy and civil liberties in its efforts to track terrorists and foreign agents.

The latest disclosure by fugitive NSA contractor Edward J. Snowden included an internal report, dated May 2012, that cited 2,776 violations over the previous year of rules meant to protect Americans' privacy. Most of the abuses involved unauthorized eavesdropping of foreigners in the United States, but more than 800 involved inadvertent collection of telephone or Internet data on Americans.

The classified materials, which were first reported by the Washington Post, make clear that the NSA did not seek to circumvent the law, and most of the abuses appear largely technical or inadvertent in nature. But one document instructed NSA analysts to carefully limit the information they provided to the Foreign Intelligence Surveillance Court, which meets in secret to review and authorize NSA requests.

The leaks came a week after President Obama vowed to restore public confidence in the NSA following months of damaging disclosures. He called on Congress to change part of the Patriot Act to provide additional safeguards over domestic intelligence operations, and he proposed creating a public advocate to challenge the government inside the secret surveillance court.

A White House spokesman, Josh Earnest, sought to allay fears that the NSA is conducting widespread unauthorized surveillance. He said Friday that the documents show the NSA is detecting and reporting potential problems, as required by law.

"This administration is committed to ensuring that privacy protections are carefully adhered to, and to continually reviewing ways to effectively enhance privacy procedures," Earnest said in a statement from Martha's Vineyard, where Obama is on vacation with his family.

Of the 2,776 violations cited, 1,904 involved cases in which a foreigner whose cellphone or email was under surveillance entered the United States, where court warrants are required for most eavesdropping. The NSA does not need a warrant to spy overseas.

But the NSA also collected emails and other communications of Americans without authorization, according to the documents.

In one case, the NSA improperly collected and commingled American and foreign emails moving through fiber-optic cables. In October 2011, months after the program had begun, the surveillance court declared it unconstitutional and ordered it shut down.

In 2008, according to the documents, a programming error confused 20, the telephone country code for Egypt, with 202, the area code for Washington, D.C. As a result, calling logs were improperly collected on a "large number" of calls.

Another document instructed NSA analysts to exclude certain information in requests to the surveillance court.

"While we do want to provide our F.A.A. overseers with the information they need, we DO NOT want to give them any extraneous information," the document said.

The F.A.A. is a reference to a law passed in 2008 that granted new authorities to the NSA in exchange for regular audits from the Justice Department and the Office of the Director of National Intelligence, and periodic reports to Congress and the surveillance court.

NSA officials held a rare on-the-record conference call with reporters Friday to defend the agency's record and its adherence to the law.

"No one at NSA thinks mistakes are OK," said John DeLong, the NSA's director of compliance. "There's no willful violation here. The fact that this document exists is actually evidence that we take each mistake very seriously."

In a separate classified briefing for House and Senate staffers, NSA officials said the mistakes reflected a tiny fraction of the 20 million emails, phone conversations and other communications that the agency searches each month, according to congressional officials who were not authorized to be quoted.

Sen. Dianne Feinstein (D-Calif.), who chairs the Senate Intelligence Committee, rose to the NSA's defense. Congress has been regularly informed about compliance problems, most of which "do not involve any inappropriate surveillance of Americans," she said.

But the Senate oversight committee "can and should do more to independently verify that NSA's operations are appropriate, and its reports of compliance incidents are accurate," she added.

Rep. Mike Rogers (R-Mich.), who chairs the House intelligence committee, vowed to reduce the errors. "Human and technical errors ... are unfortunately inevitable in any organization and especially in a highly technical and complicated system like NSA," he said.

Rep. C.A. Dutch Ruppersberger (D-Md.), ranking member on the House intelligence committee, called the violations of private rules "incredibly troubling."

"If accurate, this is outrageous, inappropriate and must be addressed," said Rep. Mike Thompson (D-St. Helena), who also serves on the intelligence committee.

"I remain concerned that we are still not getting straightforward answers from the NSA," said Sen. Patrick J. Leahy (D-Vt.), who chairs the Judiciary Committee.

Sens. Ron Wyden (D-Ore.) and Mark Udall (D-Colo.), members of the Senate intelligence committee who have been critical of the NSA, called on the White House to release more information.

"The American people have a right to know more details about the scope and severity of these violations," they said in a joint statement that called the violations "just the tip of a larger iceberg."

ken.dilanian@latimes.com