NSA DOMESTIC SURVEILLANCE FROM THE PATRIOT ACT TO THE FREEDOM ACT: THE UNDERLYING HISTORY, CONSTITUTIONAL BASIS, AND THE EFFORTS AT REFORM

Devon Ombres*

* J.D. 2006 from Stetson University College of Law; L.L.M. 2013 from American University Washington College of Law; admitted in Florida, District of Columbia, United States Court of Appeals for the 11th Circuit, and United States District Court for the Middle District of Florida.

I. INTRODUCTION

Following the September 11, 2001 attacks, America's signals intelligence community began growing exponentially in scope and power. In the forefront of this community was the National Security Agency ("NSA"), acting with the aid of the USA PATRIOT Act.[1] Between 2001 and 2013, the scope of the NSA's surveillance programs grew to include not only foreign communications, but also the mass collection of domestic metadata, including information on routing, senders, and recipients of phone calls, texts, and emails.[2]

The extent of domestic surveillance has come to light primarily through leaks of classified documents and specifically, those occurring in May 2013, by former NSA contractor, Edward Snowden.[3] The NSA is now facing unprecedented challenges to the legality of these programs from private citizens bringing Fourth Amendment actions, technology companies demanding more transparency about the demands being placed on them by Foreign Intelligence Service Court ("FISC") orders, and now Congress introducing bipartisan legislation to counteract the PATRIOT Act's provisions and the domestic surveillance that the NSA conducts.[4]

This Article will discuss the historical post-9/11 timeline relative to the domestic surveillance program. It addresses the underlying historical and constitutional concept of the Fourth Amendment, Third Party Doctrine, which the federal government is relying upon to justify the legality of mass domestic surveillance, as well as to defend legal challenges to the programs. This Article will provide an analysis of legislative proposals addressing NSA surveillance overreach, including the USA FREEDOM Act and its subsequent manager's amendment,

[1] United and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, Pub. L. No. 107–56, 115 Stat. 272 (codified as amended in scattered sections of 5, 8, 10, 12, 15, 18, 20–22, 28, 31, 42, 47, 49–50 U.S.C.).

[2] The NSA utilized contact chaining as a process of "building a network graph that models the communication . . . patte[rn]s of targeted entities . . . and their associates from the communication sent or received by the targets." OFFICE OF THE INSPECTOR GENERAL, ST-09-0002, 13 (Mar. 24, 2009), *available at* http://www.theguardian.com/world/interactive/2013/jun/27/nsa-inspector-general-report-document-data-collection [hereinafter OIG Report].

[3] Mirren Gidda, *Edward Snowden and the NSA Files—Timeline*, THE GUARDIAN (Aug. 21, 2013, 5:54PM), http://www.theguardian.com/world/2013/jun/23/edward-snowden-nsa-files-timeline.

[4] Uniting and Strengthening America by Fulfilling Rights and Ending Eavesdropping, Dragnet-collection, and Online Monitoring Act, H.R. 3361, S. 1599, 113th Cong. § 1 (2013) [hereinafter FREEDOM Act].

address their strengths and weaknesses, and discuss potential courses of legislative and judicial action to address these issues.[5] Part II of this Article addresses the timeline by which the NSA's surveillance programs were developed; Part III addresses the Third Party Doctrine under the Fourth Amendment; Part IV discusses legal challenges to the NSA surveillance programs before and after the Snowden leaks; Part V analyzes legislation proposed during the 113th Congress that addresses domestic NSA surveillance; Part VI looks at the strengths and weakness of the proposed legislation; Part VII reviews presidential action on the surveillance reforms; and Part VIII concludes this Article by discussing further judicial and legislative actions to address domestic surveillance concerns and the need to maintain a balance between privacy and security as technology advances.

II. 9/11 TO TODAY—THE DEVELOPMENT OF THE NSA'S SURVEILLANCE PROGRAMS

Immediately after the 9/11 attacks, the NSA took the first steps toward developing mass surveillance infrastructure as we know it today. First, on September 14, 2001, NSA Director General Michael Hayden approved targeted surveillance of specific, preapproved telephone numbers generating communications between the United States and foreign countries with known terrorist activities.[6] The congressional intelligence committees were made aware of these targeted collections shortly thereafter, and by October 4, 2001, authority had been granted to collect content data for such calls and emails.[7]

The NSA initially pushed back at Vice President Dick Cheney's Office's suggestion that Executive Order ("EO") 12333 permitted the data collection program to apply toward intercepting domestic communications.[8] Regardless, the program began expanding when

---

[5] *Id.*

[6] *See* OIG Report, *supra* note 2, at 3 (asserting that by September 26, 2001, the NSA anticipated collecting all telephonic metadata between the U.S. and Afghanistan).

[7] OIG Report, *supra* note 2, at 7.

[8] Exec. Order No. 12,333, Part 2.3, 3 C.F.R. 1981 (1981) (stating "*Collection of Information.* Agencies within the Intelligence Community are authorized to collect, retain or disseminate information concerning United States persons only in accordance with procedures established by the head of the agency concerned and approved by the Attorney General, consistent with the authorities provided by Part 1 of this Order . . . of the following types of information; (c) Information obtained in the course of a lawful foreign intelligence, counterintelligence, international narcotics or international terrorism investigation; (d) Information needed to protect the safety of any persons or organizations, including those who

Attorney General John Ashcroft signed off on its implementation per EO 12333 and the NSA General Counsel declared the program legal on October 5, 2001.[9]

By late 2002, the NSA was reaching out to telecommunication companies ("telecoms") to gain assistance with the surveillance program and in early 2003, installed a system at one of AT&T's San Francisco locations to collect and analyze communications data.[10] The NSA also reached voluntary agreements with three unidentified companies to share information under the program's authority, allowing it to gain access to eighty-one percent of all international telephone calls.[11] Formal letters requested information regarding communications traffic that may terminate in the United States, aggregated call record information, and computer-to-computer data.[12]

By 2004, the Federal Bureau of Investigation ("FBI") and Central Intelligence Agency ("CIA") became involved to improve collaborative analytics.[13] Despite some pushback from the telecoms, the data collection continued.[14] In 2004, Attorney General Ashcroft forwarded letters necessitating continued cooperation, stating that the law for data collection required no warrant or court order.[15] In July 2004, the FISC began issuing orders permitting the collection of metadata under the program pursuant to pen register ("PR") and trap and trace ("TT")

are targets, victims or hostages of international terrorist organizations; . . . (i) Incidentally obtained information that may indicate involvement in activities that may violate federal, state, local or foreign laws . . . .").

[9] Electronic Frontier Foundation, *Timeline of NSA Domestic Spying*, https://www.eff.org/nsa-spying/timeline (last visited Nov. 21, 2014) (citing ERIC LICHTBLAU, BUSH'S LAW: THE REMAKING OF AMERICAN JUSTICE (First Anchor Books 2009) (stating White House associates "shoved" the order in front of Ashcroft and "told him to sign it.")); *see* OIG Report, *supra* note 2, at 9, 11 (conveying that on October 11, 2001, the NSA GC for Operations and Deputy GC were read in and agreed to the program's legality).

[10] Decl. of Mark Klein, 3:5-26, Mar. 28, 2006, Jewel v. NSA, 965 F. Supp. 2d 1090 (N.D. Cal. 2013), *available at* https://www.eff.org/document/unredacted-klein-declaration.

[11] *See* OIG Report, *supra* note 2, at 27, 29–30.

[12] OIG Report, *supra* note 2, at 31.

[13] OIG Report, *supra* note 2, at 12–13.

[14] OIG Report, *supra* note 2, at 30 (showing that three companies declined to support the NSA's surveillance efforts for various reasons, including corporate liability concerns and a request to obtain an opinion from outside counsel).

[15] OIG Report, *supra* note 2, at 32. Pursuant to 18 U.S.C. § 2511(2)(a)(ii)(B) (2012), providing that no warrant or court order is required if authorization is provided by the AG, Deputy AG, Associate AG or other principal prosecuting attorney who reasonably believes that an emergency situation exists that involves conspiratorial activities threatening the national security interest. *See also* 18 U.S.C. § 2518(7)(a)(ii) (2012).

authority, and now renews the orders quarterly.[16] The domestic surveillance program's capture of purely domestic communications and the NSA's backdoor access to telecoms was revealed in 2005.[17]

On May 24, 2006, the FISC first executed an order utilizing business records as a basis for continued dragnet collection of telephone metadata as it had under prior executive authority, and continues to renew the order every ninety days.[18] Additionally, the order expanded the definition of "facility" to include gateways or cable heads through which mass communications are directed.[19] In August 2007, President Bush signed into law the Protect America Act, which gave the NSA the power to collect information if it "reasonably believed" that the surveillance target is overseas.[20] In 2008, President Bush also signed into law the Foreign Intelligence Surveillance Act ("FISA") Amendments Act, which gave retroactive immunity to telecoms that cooperated with NSA surveillance programs and provided greater authority to Attorney General Ashcroft and the Director of National Intelligence ("DNI") to conduct surveillance on citizens.[21] The collection of Internet metadata continues as domestic communications are collected "in the course of monitoring foreign

[16] Before 2006, only the presiding Foreign Intelligence Surveillance Court ("FISC") judge, Royce Lamberth and his successor, Colleen Kollar-Kotelly, were briefed on the program. OIG Report, *supra* note 2, at 25, 41. A pen register is a mechanical device that records the numbers dialed on a telephone by monitoring the electrical impulses caused when the dial on the telephone is released. It does not overhear oral communications and does not indicate whether calls are actually completed." Smith v. Maryland, 442 U.S. 735, 736, n. 1 (1979) (citing United States v. N.Y. Tel. Co., 434 U.S. 169, 169 (1977)). A "trap and trace" device is a "device or process that records the sources of incoming signals to a specific phone or computer. Often used by law enforcement as the advanced counterpart of Caller ID. A trap and trace device identifies the phone numbers or Internet addresses of incoming signals, but does not include substantive information transmitted by those signals." *See* Legal Information Institute, *Trap and Trace Device*, CORNELL UNIV. L. SCH., http://www.law.cornell.edu/wex/trap_and_trace_device (last visited Nov. 21, 2014).

[17] Eric Lichtblau & James Risen, *Spy Agency Mined Vast Data Trove, Officials Report*, N.Y. TIMES (Dec. 24, 2005), http://www.nytimes.com/2005/12/24/politics/24spy.html?pagewanted=all&_r=0; James Risen & Eric Lichtblau, *Spying Program Snared U.S. Calls*, N.Y. TIMES (Dec. 21, 2005), http://www.nytimes.com/2005/12/21/politics/21nsa.html.

[18] OIG Report, *supra* note 2, at 40.

[19] OIG Report, *supra* note 2, at 41.

[20] Protect America Act of 2007, Pub. L. No. 110–55, 121 Stat. 552 (codified as amended at 5 U.S.C. §§ 1801, 1803, 1805, 1885 (2012)); *see* James Risen, *Bush Signs Law to Widen Reach for Wiretapping*, N.Y. TIMES, Aug. 6, 2007, at A1.

[21] *See* FISA Amendments Act of 2008, Pub. L. No. 110–261, §§ 702–703, 122 Stat. 2436, 2437–38 (2008) (codified as 50 U.S.C. § 1881 (2012)); *see also* Eric Lichtblau, *Senate Approves Bill to Broaden Wiretap Powers*, N.Y. TIMES, July 10, 2008, at A1.

targets," with approximately 500 billion communication records intercepted and analyzed in 2012, via a program called "One-End Foreign," which relies on the FISA Amendments Act for its legality; this is the same year that President Obama reauthorized the FISA Amendments Act.[22]

Likewise, it was revealed that the NSA's surveillance programs expanded to include the collection of *all* domestic telephone calls as reflected in a July 13, 2013 FISC order requiring that Verizon disclose all "telephony metadata" transiting through its network on a daily basis, pursuant to 50 U.S. § 1861.[23] Similarly, a report shows that the government used the PRISM program to collect Internet data from United States service providers Microsoft, Yahoo, Google, Facebook, AOL, Skype, YouTube, and Apple and used corporate partnerships to overcome barriers to such collection.[24] Also, the MUSCULAR program tapped Yahoo and Google's cloud computing network, based overseas, to intercept entire email archives and years worth of messages and to "take a retrospective look at target activity," which can include wholly domestic communications that are simply stored out of the country.[25]

Finally, recently raised concerns include the NSA working with the National Institute of Standards and Technology ("NIST") in placing invidious backdoors into commercial Internet encryption algorithms to allow unfettered governmental access to virtually all information moving through cyberspace.[26] A top secret budget document referring to the

[22] Pub. L. No. 112–238, 126 Stat. 1631 (2012) (codified as 50 U.S.C. §§ 1801–1885 (2012)); Glenn Greenwald & Spencer Ackerman, *How the NSA is Still Harvesting Your Online Data*, THE GUARDIAN (June 27, 2013), http://www.theguardian.com/world/2013/jun/27/nsa-online-metadata-collection.

[23] *In re* the Fed. Bureau of Investigation for an Order Requiring the Prod. of Tangible Things from Verizon Bus. Network Servs. *ex rel* MCI Commc'n Servs., Inc., No. BR 13-80 (FISA Ct. 2013) (requiring Verizon to disclose "telephony metadata" pursuant to 50 U.S.C. § 1861), *available at* https://epic.org/privacy/nsa/Section-215-Order-to-Verizon.pdf.

[24] Barton Gellman & Laura Poitras, *U.S., British Intelligence Mining Data from Nine U.S. Internet Companies in Broad Secret Program*, WASH. POST (June 7, 2013), http://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html.

[25] Barton Gellman & Ashkan Soltani, *NSA Infiltrates Links to Yahoo, Google Data Centers Worldwide, Snowden Documents Say*, WASH. POST (Oct. 30, 2013), http://www.washingtonpost.com/world/national-security/nsa-infiltrates-links-to-yahoo-google-data-centers-worldwide-snowden-documents-say/2013/10/30/e51d661e-4166-11e3-8b74-d89d714ca4dd_story.html.

[26] Jeff Larson, Nicole Perlroth, & Scott Shane, *Revealed: The NSA's Secret Campaign to Crack, Undermine Internet Security*, PROPUBLICA (Sept. 5, 2013, 2:08 PM),

SIGINT (signals intelligence) Enabling Project gives this credence, as it reflects a $250 million annual layout toward goals of inserting vulnerabilities in commercial encryption systems, influencing policies, standards and specifications for commercial public key technologies, and collecting data or metadata from cooperative networks or increased control over networks.[27]

III. THE FOURTH AMENDMENT THIRD PARTY DOCTRINE AND MASS DATA COLLECTION

There is little doubt that the collection of content data, absent probable cause, violates the Fourth Amendment as an unreasonable search.[28] However, whether the mass collection of domestic metadata violates the Fourth Amendment is a question that is still being wrestled with due to the historical approval of the Third Party Doctrine ("TPD") arising from the seminal opinion of *Smith v. Maryland*.[29]

In *Smith*, a PR was used to assist in a conviction of a burglary.[30] The Supreme Court held that using a PR did not constitute an unreasonable search because individuals are aware that phone companies maintain permanent records of dialed phone numbers, thereby abrogating any expectation of privacy.[31] As *Smith* has not been overruled, it maintains its standing as a guiding principle under *stare decisis* and is being utilized, at least in part, as a basis for conducting domestic surveillance as discussed below.

The FISC cites directly to the *Smith* reasoning, in a heavily redacted

http://www.propublica.org/article/the-nsas-secret-campaign-to-crack-undermine-internet-encryption (explaining that the NIST creates and standardizes Internet encryption algorithms and codes for widespread use in commercial telecommunication and e-communication products).

27 SIGINT Enabling Project, *Top Secret//SI/TK//NOFORN*, 115–17, PROPUBLICA, *available at* http://www.propublica.org/documents/item/784285-sigint-enabling-project.html.

28 *See* United States v. Warshak, 631 F.3d 266, 286 (6th Cir. 2010) ("Over the last decade, email has become 'so pervasive that some persons may consider [it] to be [an] essential means or necessary instrument[ ] for self-expression, even self-identification.' It follows that email requires strong protection under the Fourth Amendment; otherwise, the Fourth Amendment would prove an ineffective guardian of private communication, an essential purpose it has long been recognized to serve.") (citations omitted).

29 442 U.S. 735 (1979).

30 18 U.S.C. § 3127(3) (2012) (defining pen register as a device that records dialing, routing, addressing, or signaling information by an instrument or facility from which a wire or electronic communication is transmitted); *Smith*, 442 U.S. at 737.

31 *Smith*, 442 U.S. at 743–45 (citing United States v. Miller, 425 U.S. 435, 442 (1976)).

opinion/order, in noting that there is no reasonable expectation of privacy in the collection of metadata.[32] The FISC notes that Congress relaxed requirements to collect "non-content addressing information through [PR] and [TT] devices" through the PATRIOT Act and FISA Amendments and that "such information is not protected by the Fourth Amendment."[33] Like phone calls under *Smith*, the FISC held that email users, due to the same reasoning, also do not have an expectation of privacy.[34] The FISC recognized the need for only a relevance standard, rather than reasonable suspicion, in approving the government's requests for widespread surveillance.[35]

The FISC analogizes the low hit rate in obtaining actionable information through dragnet metadata collection to DUI checkpoints and drug testing students in justifying suspicionless searches.[36] Further, great deference must be given to the government officials who have a unique understanding of these situations, and they do not need to act in the least intrusive means available.[37] In so approving of the bulk collection of metadata, the court provided:

> analogous to suspicionless searches and seizures that have upheld under the Fourth Amendment in that the Government's need is compelling and immediate, the intrusion on individual privacy interests is limited, and bulk collection appears to be a reasonably effective means of monitoring (redacted) related operatives . . . . In these circumstances, the certification of relevance is consistent with the fact that only a very small proportion of the huge volume of information collected will be directly relevant to the FBI's (redacted)

---

[32] *Case Name and Number Redacted*, at 58–59 (FISA Ct. Date Redacted) (executed by FISC Presiding Judge Colleen Kollar-Kotelly), *available at* http://www.dni.gov/files/documents/1118/CLEANEDPRTT%201.pdf [hereinafter *FISC Opinion*].

[33] 18 U.S.C. § 3127(4) (2012) (defining a "trap and trace device" as a device that captures incoming electronic or other impulses that identify the originating number or other information that identifies the source of a wire or electronic communication); *FISC Opinion*, *supra* note 32, at 19.

[34] *FISC Opinion*, *supra* note 32, at 19.

[35] *FISC Opinion*, *supra* note 32, at 29 (citing 147 CONG. REC. S10990,11003 (daily ed. Oct. 25, 2001) (statement of Sen. Leahy) ("[T]he FBI 'made a clear case that a relevance standard is appropriate for counterintelligence and counterterrorism investigations.'")).

[36] *FISC Opinion*, *supra* note 32, at 50–52 (citing Bd. of Educ. of Indep. Sch. Dist. No. 92 v. Earls, 536 U.S. 822 (2008) (discussing drug testing students)); Mich. Dep't. of State Police v. Sitz. 496 U.S. 444 (1990) (discussing DUI checkpoints).

[37] *FISC Opinion*, *supra* note 32, at 53.

investigations.[38]

IV. LEGAL CHALLENGES TO DOMESTIC SURVEILLANCE AND JUDICIAL PUSHBACK ON THE THIRD PARTY DOCTRINE

A. Pre-Snowden Leak Cases

Several challenges to the NSA's domestic surveillance programs have been made against both the government and private entities working with the government. These include *Hepting v. AT&T*,[39] *Jewel v. NSA*,[40] and *Al-Haramain Islamic Foundation v. Bush*,[41] all of which sought redress for Fourth Amendment violations under the NSA's surveillance programs. In *Hepting*, the Electronic Frontier Foundation ("EFF") sought to preclude AT&T from routing copies of Internet traffic directly to the NSA.[42] In *Jewel*, numerous individuals brought actions against the NSA to cease the ongoing dragnet collection of metadata.[43] In *Al-Haramain*, plaintiffs, a now defunct Islamic organization, sued the Bush administration for alleged warrantless wiretapping of the Foundation, which they asserted violated FISA.[44]

In all three cases, the government moved to dismiss the actions by asserting that the State Secrets Privilege preempted litigation.[45] In what

---

[38] *FISC Opinion*, *supra* note 32, at 54.

[39] Hepting v. AT&T Corp., 439 F. Supp. 2d 974 (N.D. Cal. 2006), *cert. denied*, Ctr. for Constitutional Rights v. Obama, 13 S. Ct. 1497 (2014).

[40] Jewel v. NSA, No. C 08-cv-4373 VRW, 2010 U.S. Dist. LEXIS 5110 (N.D. Cal. Jan. 10, 2010), *cert. denied*, Ctr. for Constitutional Rights v. Obama, 13 S. Ct. 1497 (2014).

[41] Al-Haramain Islamic Found., Inc. v. Bush (*In re* NSA Telecomms. Records Litig.), 633 F. Supp. 2d 949 (N.D. Cal. 2009), *cert. denied*, Ctr. for Constitutional Rights v. Obama, 13 S. Ct. 1497 (2014); Al-Haramain Islamic Found., Inc. v. Bush, 451 F. Supp. 2d 1215 (D. Or. 2006), *cert. denied*, Ctr. for Constitutional Rights v. Obama, 13 S. Ct. 1497 (2014).

[42] *Hepting*, 439 F. Supp. 2d at 974; *see also In re* NSA Telecomms. Records Litig., 633 F. Supp. 2d 892 (N.D. Cal. 2007) (discussing the efforts of state officials to compel telecommunication carriers to release information regarding the disclosure of telecommunication records to the NSA).

[43] *See Hepting*, 439 F. Supp. 2d at 974; *see also In re* NSA Telecomms. Records Litig., 633 F. Supp. 2d 892 (discussing the efforts of state officials to compel telecommunication carriers to release information regarding the disclosure of telecommunication records to the NSA); Complaint for Jewel, Jewel v. NSA, No. C 08-cv-4373 VRW, 2010 U.S. Dist. LEXIS 5110 (N.D. Cal. Jan. 10, 2010); *see also*, Electronic Frontier Found., *Jewel v. NSA*, https://www.eff.org/cases/jewel (last visited Nov. 21, 2014).

[44] *Al-Haramain Islamic Found., Inc.*, 633 F. Supp. 2d 949; *Al-Haramain Islamic Found., Inc.*, 451 F. Supp. 2d 1215.

[45] Doc. No. 308 at 3, Hepting v. AT&T Corp., No. C-06-672-VRW, 2006 U.S. Dist. LEXIS 41160 (N.D. Cal. 2006) (explaining that the United States Government sought dismissal or summary judgment based on the state secrets privilege in May 2006); *see*

turned out to be a pyrrhic victory, the courts rejected the State Secrets Privilege argument as abrogated by 50 U.S.C. § 1806.[46] However, none of the plaintiffs have yet been successful in having their cases decided on the merits.[47] The district court dismissed *Hepting* because of the FISA Amendments of 2008 that granted retroactive immunity to telecoms, and the Ninth Circuit upheld the dismissal.[48] The district court dismissed *Jewel* on the statutory claims for damages under FISA and for injunctive relief on sovereign immunity grounds, although the Fourth Amendment question may yet survive.[49] In *Al-Haramain*, the district court granted a summary judgment award of $2.5 million in damages. The Ninth Circuit reversed and dismissed that judgment, holding that the government did not waive sovereign immunity and that to be individually liable under 50 U.S.C. § 1810, the governmental official subject to the claim must also be subject to criminal prosecution.[50]

In the most high profile case, *Clapper v. Amnesty International*

Government Defendant's Motion to Dismiss and for Summary Judgment, Doc. No. 18, Jewel v. NSA, No. C:08-cv-4373-VRW, 2010 U.S. Dist. LEXIS 5110 (N.D. Cal. Jan. 10, 2010); *see also* Kurt Opshal, *Breaking News: Court Holds That FISA Preempts State Secret Privilege*, ELECTRONIC FRONTIER FOUND. (July 2, 2008), https://www.eff.org/deeplinks/2008/07/court-rules-fisa-preempts-state-secret-privilege (explaining the Northern District of California held that the FISA Act preempted the State Secrets Privilege in *Al Haramain v. Bush*). The State Secrets Privilege is one that must be formally asserted by the head of the department with control over the matter, and the Court must do without forcing the disclosure of the privileged information. The government may not be required to divulge the information for an *in camera* inspection by the court if the judge finds, based on "all the evidence and circumstances" that there is a reasonable danger that such disclosure would "expose military matters, which in the interest of national security, should not be divulged." United States v. Reynolds, 345 U.S. 1, 9–10 (1953).

[46] 50 U.S.C. § 1806(f) (2012) provides that if the disclosure of documents subject to a legal challenge would harm national security, same may be reviewed *ex parte* and *in camera* by the court; *see also*, Jewel v. NSA, 965 F. Supp. 2d 1090, 1105 (N.D. Cal. 2013); *Hepting*, 2006 U.S. Dist. LEXIS 41160, at *10; Opshal, *supra* note 45 (referencing the Northern District of California's ruling that the FISA Act preempted the State Secrets Privilege in *Al-Haramain v. Bush*).

[47] *Jewel*, 965 F. Supp. 2d at 1097; Al-Haramain Islamic Found., Inc. v. Obama, 705 F.3d 845, 855 (9th Cir. 2012); NSA Telecomms. Records Litig. v. AT&T Corp., 671 F.3d 881 (9th Cir. 2011).

[48] *NSA Telecomms. Records Litig.*, 671 F.3d 881, *cert denied*, Hepting v. AT&T Corp., 133 S. Ct. 421 (2012).

[49] *Jewel*, 965 F. Supp. 2d at 1097.

[50] "An aggrieved person . . . who has been subjected to an electronic surveillance . . . in violation of [50 U.S.C. § 1809] shall have a cause of action against any person who committed such violation . . . ." 50 U.S.C. § 1810 (2012); *Al-Haramain Islamic Found., Inc.*, 705 F.3d at 855.

USA,[51] a number of international groups sought to have Section 702 of the FISA Amendments Act, 50 U.S.C. § 1881(a), declared facially unconstitutional as violating the Fourth Amendment by asserting that surveillance on their international activities compromised their ability to "locate witnesses, cultivate sources, obtain information, and communicate confidential information to their clients."[52] The Supreme Court did not address the Fourth Amendment claims, but did hold that the plaintiffs lacked standing as they could not prove injury in fact because neither speculation of surveillance nor taking action to avoid surveillance constitutes injury to warrant standing.[53]

B. Post-Snowden Leak Challenges and Recent Developments

Despite the above, the Supreme Court indicated a potential willingness to address whether various methods of electronic surveillance violated the Fourth Amendment in *United States v. Jones*, a case involving the placement of a GPS tracker on a suspect's vehicle.[54] In a concurring opinion, Justice Sotomayor suggested a need to revisit the TPD in the digital age in the concurring opinion and noted that electronic monitoring of individuals can chill associational and expressive freedoms and that the government's unfettered access to substantial intimate information "may alter the relationship between citizen and government that is inimical to democratic society."[55] Further, it may be "necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties" as that expectation is ill suited to the digital age due to the massive amounts of information disclosed "in the course of carrying out mundane tasks."[56] Information disclosed to a third party for a limited purpose should not be disentitled to Fourth Amendment protections simply because as it stands, secrecy is a prerequisite for privacy.[57]

It is increasingly obvious that the court's reliance upon the concept that data is voluntarily disseminated is misplaced because of the reality

---

[51] 133 S. Ct. 1138 (2013).

[52] *Id.* at 1145; *see* 50 U.S.C. § 1881(a) (2012).

[53] *Clapper*, 133 S. Ct. at 1150–51.

[54] 132 S. Ct. 945 (2012).

[55] *Id.* at 956 (Sotomayor, J., concurring) (quoting United States v. Cuevas-Perez, 640 F.3d 272, 285 (7th Cir. 2011) (Flaum, J., concurring)).

[56] *Id*. at 957.

[57] *Id.* (citing Smith v. Maryland, 442 U.S. 735, 749 (1979) (Marshall, J., dissenting) ("Privacy is not a discrete commodity, possessed absolutely or not at all.")).

that post-modern usage of the Internet is to conduct one's necessary daily activities, fostering arguments toward the fundamental right of access to the Internet.[58] There is no longer a dichotomy between voluntary and involuntary relinquishment of electronic information due to the ubiquity of e-communication, rendering untenable any construction of the Fourth Amendment that makes unreasonable the expectation of privacy through such communication.[59] The Court recognized this distinction in *City of Ontario v. Quon*,[60] holding:

> Rapid changes in the dynamics of communication and information transmission are evident not just in the technology itself but in what society accepts as proper behavior . . . . Cell phone and text message communications are so pervasive that some persons may consider them to be essential means or necessary instruments for self-expression, even self-identification. *That might strengthen the case for an expectation of privacy.*[61]

The Court seems to note that just because the way of life is changing does not result in the loss of fundamental liberties, and as interactions with third parties are fundamental to life in a technological era, invocation of the TPD should be limited.[62] This apparent trend of the Court toward a more limited interpretation of the Fourth Amendment via technological developments is, to a degree, corroborated by their recent holding in *Riley v. California*, prohibiting the police from accessing the digital data stored in a defendant's cellular phone incident to arrest.[63] The Court declined to extend *Smith* to allow officers to examine a cell phone's call logs.[64]

In that vein, Judge Richard Leon of the United States District Court for the District of Columbia recently entered an order granting a preliminary injunction prohibiting the NSA from continuing its ongoing bulk collection of metadata in *Klayman v. Obama*.[65] The court found that the plaintiff, Larry Klayman, had standing to challenge both the NSA's

---

[58] Saby Ghoshray, *Privacy Distortion Rationale for Reinterpreting the Third Party Doctrine of the Fourth Amendment*, 13 FLA. COASTAL L. REV. 33, 74–75 (2011).

[59] *Id.* at 74.

[60] 130 S. Ct. 2619, 2629–30 (2010).

[61] *Id.* (emphasis added).

[62] *See* Ghoshray, *supra* note 58, at 80, 83.

[63] 134 S. Ct. 2473, 2485 (2014).

[64] *Id.* (citing Smith v. Maryland, 442 U.S. 735, 743–45 (1979)).

[65] *See* Klayman v. Obama, 957 F. Supp. 2d 1 (D.D.C. 2013) (automatically staying the temporary injunction was automatically due to national security concerns pending the outcome of appeals), *available at* http://online.wsj.com/public/resources/documents/JudgeLeonNSAopinion12162013.pdf.

collection of metadata, and its analysis thereof in contravention of *Clapper*; the government set forth an argument detailing the "historical repository . . . of terrorist-related communications *across multiple telecommunications networks*" and the creation of a "*comprehensive* metadata database."[66]

Judge Leon reasoned that the plaintiffs had a likelihood of success on the merits of their Fourth Amendment claims because the FISC's reliance on *Smith* is misplaced due to the "evolutions in the Government's surveillance capabilities, citizens' phone habits, and the relationship between the NSA and telecom companies," and that the "surveillance program now before [the court] is so different from a simple pen register that *Smith* is of little value."[67] In so holding, the court addressed the plurality in *Jones*, as well as that in *Quon*, in denoting that an increasing dependency on technology for everyday activities creates a greater and more reasonable expectation of privacy in cell phone use as metadata "reflects a wealth of detail about [individuals'] familial, political, professional, religious, and sexual associations."[68] Moreover, it is likely that the plaintiffs will be able to show that the collection of bulk metadata constitutes an unreasonable search because "no court has ever recognized a special need sufficient to justify continuous, daily searches of virtually every American citizen without any particularized suspicion."[69]

Shortly after the *Klayman* Order was entered, Judge William Pauley entered a diametrically opposed Order in *American Civil Liberties Union*

---

[66] *Id.* at 37–38.

[67] *Id.* at 45, 47 (Additional differences between the scenario of *Smith* and bulk metadata collection include the short term nature of the pen register versus the creation of a database containing at least five years worth of historical information, the creation of a formal partnership between the NSA and telecoms whereby the latter provide daily rolling updates of all metadata moving through the networks, the "almost-Orwellian" technology that allows for the storage of such metadata for analysis, and the nature and quantity of individuals' collected metadata differs significantly from that collected in 1979 under the guidance of *Smith*.).

[68] *See id.* at 52–55 (discussing United States v. Jones, 132 S. Ct. 945, 955–56 (2012) (Sotomayor, J., concurring), 962 (Alito, J., concurring)); Ontario v. Quon, 130 S. Ct. 2619, 2630 (2010).

[69] *Klayman*, 957 F. Supp. 2d at 56–58 (citing Nat'l Fed'n Of Emps.-IAM v. Vilsack, 681 F.3d 483, 488–89 (D.C. Cir. 2012) (noting that warrantless searches are *per se* unreasonable under the Fourth Amendment absent some quantum of individualized suspicion); Bd. of Educ. v. Earls, 536 U.S. 822, 830–34 (2002) (noting that context specific inquiries can merit suspicionless searches upon consideration of the nature of the privacy interests compromised, the character of the intrusion, and the nature and immediacy of the governments concerns and whether the search will meet them.).

("ACLU") *v. Clapper*,[70] in the Southern District of New York. Therein, Judge Pauley held that the ACLU was precluded from bringing a statutory claim against Section 215 of the Patriot Act.[71] More to the point, Judge Pauley explicitly disagreed with the *Klayman* court in holding that until the Supreme Court deemed otherwise, the *Smith* precedent must hold and noted that "[t]he collection of breathtaking amounts of information unprotected by the Fourth Amendment does not transform that sweep into a Fourth Amendment search."[72]

Regardless of Judge Pauley's ruling in *ACLU*, Judge Leon's novel opinion in *Klayman* is the first instance of a court even making a preliminary finding that the NSA domestic surveillance program is unconstitutional. These opinions are clearly not the final word on the matter, and there is little doubt that both will be appealed to the Supreme Court. The timing of such appeals is questionable. Should the appeals take the traditional route, it may be some time before the Supreme Court speaks on either case, unless either are accepted on a petition for certiorari before judgment. *ACLU v. Clapper* was argued before the Second Circuit Court of Appeal on September 2, 2014, and *Klayman v. Obama* had not yet been argued.[73] As of September 2014, no opinion for either case has been issued by the circuit courts.

V. PROPOSED LEGISLATIVE REMEDIES TO MASS DOMESTIC SURVEILLANCE

With the limited efficacy in challenging the NSA's domestic surveillance programs in the courts, it is up to Congress to rein in the NSA overreach. Despite significant concern in the private sector for years regarding perceived governmental overreach via NSA surveillance, bipartisan congressional support for greater transparency, oversight, and reform of the intelligence community did not emerge until Mr. Snowden began leaking classified documents exposing the breadth and depth of government surveillance.[74]

---

[70] 959 F. Supp. 2d 724 (S.D.N.Y. 2013).

[71] *Id*. at 741 (citing Block v. Cmty. Nutrition Inst., 467 U.S. 340 (1984)).

[72] *Id*. at 752.

[73] *ACLU v. Clapper—Challenge to NSA Mass Call-Tracking Program*, AM. CIVIL LIBERTIES UNION, https://www.aclu.org/national-security/aclu-v-clapper-challenge-nsa-mass-phone-call-tracking (last visited Dec. 16, 2014); *Argument Calendar, Courtroom 1703*, U.S. CT. OF APPEALS FOR THE SECOND CIRCUIT, http://ww2.ca2.uscourts.gov/calendar/index.php?eID=380 (last visited Dec. 16, 2014).

[74] Associated Press, *House Passes NSA Regulations, First Legislation Since Snowden*

Prior to the Snowden leaks beginning in May 2013, the extent to which Congress was aware of the scope of the NSA's surveillance program was likely limited. The Senate Select Committee on Intelligence and the House Permanent Select Committee on Intelligence received full briefings, but other members briefed did not have the benefit of staff expertise to analyze the extensive program documentation.[75]

There is little doubt that the NSA's surveillance programs are overbroad, and it is collecting far more data than limited targeting would suggest. However, few would argue against the importance of targeted collection in a counterterrorism capacity. Thus, Congress's first effort at addressing the NSA surveillance program may not necessarily have stricken an appropriate balance between Fourth Amendment protections and counterterrorism intelligence gathering needs, although recent efforts have gained more traction.

A. House Bills and Actions

i. The Amash-Conyers Amendment

Congress's first major effort to address the NSA's overreach came during the Department of Defense Appropriations Act debate via the Amash-Conyers Amendment. The Amendment would have precluded funding for any surveillance conducted by the NSA not explicitly falling under the purview of 50 U.S.C. §1861, also known as Section 215 of the PATRIOT Act, regarding the investigation of a suspected agent of a foreign power.[76] The Amendment was the subject of heated debate.

Leaks, CBSDC (May 22, 2014, 2:06 PM), http://washington.cbslocal.com/2014/05/22/house-passes-nsa-regulations-first-legislation-since-snowden-leaks/.

[75] *See* Glenn Kessler, *Obama's Claim that 'Every Member of Congress' was Briefed on Telephone Surveillance*, WASH. POST FACT CHECKER (June 11, 2013, 6:00 AM), http://www.washingtonpost.com/blogs/fact-checker/post/obamas-claim-that-every-member-of-congress-was-briefed-on-telephone-surveillance/2013/06/10/fd03ea8e-d21f-11e2-8cbe-1bcbee06f8f8_blog.html (relaying that Senator Jeff Merkley stated he needed special permission to be briefed on the issue, not serving on the Intelligence Committee and conveying that Representative Keith Ellison noted tackling the issue in depth required staff assistance).

[76] H.R. 2397, 113th Cong. § 1 (2013); H. Amend. 100 to H.R. 2397, 113th Cong. § 1 (2013) ("None of the funds made available by this Act may be used to execute a [FISC] order pursuant to section 501 of [FISA] of 1978 (50 U.S.C § 1861) that does not include the following sentence: 'This Order limits the collection of any tangible things [including metadata] that may be authorized to be collected pursuant to this Order to those tangible things that pertain to a person who is subject of an investigation described in [50 U.S.C. § 1861]'") (Rep. Justin Amash (R), Rep. John Conyers Jr. (D)). Section 215 is widely regarded as providing the basis through which surveillance overreach occurs by requiring disclosure of tangible evidence via an Order specifying that the information sought is part and parcel to an

Proponents argued that it would end abuse of Section 215 while allowing legitimate investigations to continue.[77] Opponents argued that this was the wrong vehicle to address the issue. They argued that the NSA program was constitutional because it did not access communication content and it was necessary to continue battling terrorism.[78]

The Amash-Conyers Amendment came as somewhat of a surprise to House members and shredded party lines by bringing together liberal Democrats and Tea Party Republicans on both sides of the vote, but ultimately failed in a vote of 217–205.[79] At the time of the vote, members had not yet conducted a full analysis of the issue and likely wanted to hold hearings to determine how to best address the NSA programs before simply cutting off funding.

ii. The USA FREEDOM Act—Introduced Version

Representative Jim Sensenbrener, a Republican and the primary sponsor of the USA PATRIOT Act, has introduced the comprehensive USA FREEDOM Act to counteract the perceived NSA overreach occurring through the implementation of Section 215.[80] On introduction, it had 102 bipartisan cosponsors, and Senator Patrick Leahy's companion bill in the Senate, Senate Bill 1599, has eighteen bipartisan cosponsors.[81] The House of Representatives passed this bill with amendments that are

"authorized investigation . . . to protect against international terrorism. It is titled "Access to certain business records for foreign intelligence and international terrorism investigations," and it provides, in part:

"(a)(1) The Director of the [FBI] . . . may make an application for an order requiring the production of any tangible things . . . for an investigation to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution.

(2) An investigation conducted under this section shall –(A) be conducted under guidelines approved by the Attorney General under Executive Order 12333." 50 U.S.C. § 1861(a)(1)(2).

[77] *See* 159 CONG. REC. H4981, 5023–25 (statements of Reps. Justin Amash, John Conyers, Jr., James Sensenbrenner) (daily ed. July 24, 2013).

[78] *Id.* at 5024 (statements of Reps. Bill Young, Mike Rogers, and Michelle Bachmann).

[79] *Id.* at 5028 (tallying the Yea votes that included Rep. Alan Grayson (D) and Rep. Raul Labrador; Nay votes included Rep. Chris Van Hollen (D) and Rep. Michelle Bachmann).

[80] *See* H.R. 3361, 113th Cong. (2013), *available at* https://www.congress.gov/bill/113th-congress/house-bill/3361/cosponsors?q=%7B%22search%22%3A%5B%22hr+3361%22%5D%7D.

[81] *See id.*; *see also* S. 1599, 113th Cong. (2013), *available at* https://www.congress.gov/bill/113th-congress/senate-bill/1599/cosponsors?q=%7B%22search%22%3A%5B%22s+1599%22%5D%7D.

discussed in more detail below.[82]

The FREEDOM Act takes several steps to enact reforms to the PATRIOT and FISA Amendment Acts. This includes placing stronger requirements on obtaining FISC Orders for the production of information by removing the presumption of relevance from any request and precluding production for mere threat assessments.[83] Likewise, it prohibits the placement of PR and TT devices by precluding their use for threat assessments and by requiring specificity in any request for such devices.[84] It also places minimization requirements on the use of such devices for conducting surveillance by prohibiting the retention or dissemination of information collected not pertaining to a target of the search; for example, the NSA must enact procedures to discard any dragnet information collected not correlated to targeted and approved searches.[85]

Title III of the Act directly addresses Section 702 of FISA, 50 U.S.C. § 1881(a), by prohibiting a search of a collection of communications of a "United States person" unless an emergency authorization is granted.[86] It also limits collecting communications information occurring within the United States by limiting such to targeted individuals or those with a targeted account identifier.[87] It also strengthens, to a lesser degree, prohibitions against reverse targeting of United States citizens by setting forth that "a significant purpose" of foreign targeting cannot be to obtain communications from a United States person.[88]

The FREEDOM Act also improves transparency of surveillance in several ways. It requires that the Department of Justice ("DOJ") release opinions, in full, redacted, or as summaries, issued by the FISC from 2003 forward that include a significant construction or interpretation of law describing the issue of law and basis of the decision.[89] Second, it permits telecoms to disclose quarterly estimates of the number of orders received

---

[82] The House passed H.R. 3361 on Roll Call Vote No. 230 by a vote of 303–121. 160 CONG. REC. H4789, 4789–93 (2014).

[83] H.R. 3361 § 101 (amending 50 U.S.C. § 1861(b)).

[84] *Id.* at § 201 (amending 50 U.S.C. § 1842(c)).

[85] *Id.* at § 202 (amending 50 U.S.C. § 1842).

[86] *Id.* at § 301 (amending 50 U.S.C. § 1881a(b)).

[87] *Id.* (amending 50 U.S.C. § 1881a(d) & (i)).

[88] H.R. 3361 § 303 (as introduced) (amending 50 U.S.C. § 1881a(b)), *available at* https://www.congress.gov/bill/113th-congress/house-bill/3361/text/162269?q={%22search%22:[%22hr%203361%22]}.

[89] *Id.* at § 4 (amending Title IX, § 905).

and complied with and the number of accounts affected.[90] Last, it requires annual disclosure of orders applied for and granted and the number of United States persons targeted.[91]

The Act, as introduced, proposed the creation of an "Office of the Special Advocate" that would act as counsel to entities against which Orders to Produce are sought and will represent such entities before the FISC.[92] This section of the bill would also create a right to appeal FISC decisions before a review panel, which would examine the issue under *de novo* review.[93]

iii. Other House Bills

A number of smaller bills that address limited aspects of the FREEDOM Act have been introduced in the House, but none have the extensive and bipartisan support thereto afforded. One such bill, the Surveillance State Repeal ("SSR") Act, does exactly as its name indicates in fully repealing the PATRIOT and 2008 FISA Amendments Acts, requiring instead that a probable cause warrant be issued to collect information on United States persons and requiring stronger whistleblower protections.[94] Another bill that has received attention, the Intelligence Oversight and Accountability Act, essentially only requires greater reporting to Congress on orders before the FISC and affords no public transparency.[95] A third, the Government Surveillance Transparency Act, allows the disclosures sought by technology companies by permitting the release of the aggregate number of FISC orders with which they were required to comply.[96] The Telephone Surveillance Accountability Act only increases the standard by which an order for a search of telephone metadata is granted from relevance to a "reasonable articulable suspicion."[97]

[90] *Id.* at § 604 (as referred in the Senate) (amending 50 U.S.C. § 1862(b)) (In H.R. 3361, as introduced, the disclosure limitations were set forth in § 601).

[91] *Id.* at § 602 (as referred in the Senate).

[92] *Id.* at § 401 (establishing the Office of the Special Advocate and Title IX, "The Office of the Special Advocate," in 50 U.S.C. §§ 1801-1885).

[93] *Id.* (establishing the Office of the Special Advocate).

[94] *See* H.R. 2818, 113th Cong. (2013).

[95] H.R. 3103, 113th Cong. § 2 (2013).

[96] H.R. 2736, 113th Cong. § 901 (2013).

[97] H.R. 2684, 113th Cong. § 2 (2013).

B. Comprehensive Senate Bills and Actions

A companion bill to the original USA FREEDOM Act was introduced in the Senate as Senate Bill 1599, but has since been updated by Senator Patrick Leahy as Senate Bill 2685 following passage of the Act in the House.[98] In addition to the USA FREEDOM Act, Senator Ron Wyden and Senator Diane Feinstein have introduced two comprehensive bills to address NSA surveillance, the Intelligence Oversight and Surveillance Reform Act and the FISA Improvements Act, respectively.[99] Senator Wyden's bill is substantially similar to the FREEDOM Act with some ancillary addendums. For instance, it provides additional protections to ensure that no records obtained extrajudicially from an order will be admissible in court.[100] It significantly addresses reverse targeting of United States persons and requires greater disclosure of FISA orders.[101] It also addresses the Supreme Court's holding in *ACLU* by creating a cause of action to challenge government surveillance via a reasonable belief that communications will be collected and reasonable steps were taken to avoid surveillance.[102]

Conversely, Senator Feinstein's bill, which passed out of the Senate Select Committee on Intelligence, has been much derided for essentially codifying the NSA's conduct of the past decade.[103] While there is a section titled "General Prohibition on Bulk Collection," it actually allows for metadata collection upon identifying the facility from which it will be collected and using minimization procedures relative to who can utilize the records and how, but annual aggregated numbers of investigative

98 S. 2685, 113th Cong. § 2 (2014); S. 1599, 113th Cong. § 1 (2013).

99 S. 1631, 113th Cong. § 1 (2013); S. 1551, 113th Cong. § 1 (2013).

100 S. 1551 §§ 101–02 (amending sections entitled "Privacy Protections for Section 215 Business Records Orders" and "Emergency Authority for Access to Call Data Records," respectively).

101 *Id.* at §§ 302, 406 (amending section entitled "Protections Against Collection of Wholly Domestic Communications not Concerning Terrorism under FISA Amendment Act" and adding section entitled "Disclosure," respectively).

102 *Id.* at § 305 (amending section entitled "Challenges to Government Surveillance").

103 S. REP. NO. 113–119, at 12 (2013); John Hudson & Shane Harris, *Diane Feinstein is Still a Friend of the NSA*, FOREIGN POLICY, (Oct. 31, 2013, 6:21 PM), http://thecable.foreignpolicy.com/posts/2013/10/31/diane_feinstein_is_still_a_friend_of_the_nsa_after_all; Matt Sledge, *Senate Intelligence Committee Passes Bill That Codifies, Expands NSA Powers*, HUFFINGTON POST (Oct. 31, 2013, 4:30 PM), http://www.huffingtonpost.com/2013/10/31/senate-bill-nsa_n_4183183.html; Trevor Timm, *Sen. Diane Feinstein's New NSA Bill Will Codify and Extend Mass Surveillance of Americans*, ELECTRONIC FRONTIER FOUND. (Oct. 31, 2013), https://www.eff.org/deeplinks/2013/10/sen-feinsteins-nsa-bill-will-codify-and-extend-mass-surveillance.

leads, warrants, and court orders would be publicly released.[104] To a degree, it provides for greater congressional oversight by requiring semiannual Attorney General reports and an annual Director of National Intelligence report on violations of the law or executive order and by providing access to all FISC orders to the congressional intelligence committees and other members of Congress.[105] However, it does not provide for additional public transparency.[106]

Another piece of the bill limits targeting of foreign nationals entering the United States to an additional seventy-two hours, which has been subject to abuse.[107] Lastly, two improvements to the current surveillance regime allow the FISC to appoint amicus counsel to address novel issues before it and increase criminal penalties for gaining unauthorized access to data collected under the FISA surveillance programs.[108]

i. USA FREEDOM Act

The updated Senate version, Senate Bill 2685, of the USA FREEDOM Act is trimmed down as well and maintains differences with the House passed iteration of the Act, House Bill 3361. Notably, House Bill 3361 provides broader leeway in obtaining information and call data through the use of specific selection terms.[109] Under Senate Bill 2685, applying to the FISC for a search requires a factual statement reflecting that foreign powers or agents thereto are engaging in "international terrorism or activities in preparation therefor," while House Bill 3361 only requires a showing that such a search relates to foreign powers.[110] House Bill 3361 specifically references the need to "protect against international terrorism," after defining the necessary showing to grant an application, but the Senate's more exacting language appears to close a

104 S. REP. NO. 113–119 § 2 (discussing section entitled "Supplemental Procedures for Acquisitions of Certain Business Records for Counterterrorism Purposes").

105 *See id.* at § 2; S. 1631, 113th Cong. §§ 509, 601–2 (2013) (discussing sections entitled "Annual Reports on Violations of Law or Executive Order," "Semiannual Report of the Attorney General," and "Availability of Reports and Submissions," respectively).

106 *Id.*

107 *Id.* at § 7 (discussing section entitled "Temporary Targeting of Persons other than United States Persons Traveling into the United States").

108 *Id.* at §§ 3–4 (discussing sections entitled "Enhanced Criminal Penalties for Unauthorized Access to Collected Data" and "Appointment of Amicus Curiae," respectively).

109 *Compare* S. 2685, 113th Cong. § 101(a) (2014), *with* H.R. 3361, 113th Cong. § 101(a) (2013) (as referred in the Senate).

110 *Compare* S. 2685 § 101(a), *with* H.R. 3361 § 101(a).

loophole that could conceivably be utilized to collect additional metadata.[111]

Additionally, Senate Bill 2685, in Title I, FISA Business Records Reform, creates a more exacting definition in furtherance of minimization procedures by including a subsection applying such procedures to persons not the subject of authorized investigations or in contact with such persons or who are not suspected agents of foreign powers.[112] A similar section is not contained in the version of House Bill 3361 that was passed in the House.[113]

The concern regarding overly broad or undefined terms under the context of "specific selection term" is somewhat abrogated in Senate Bill 2685. Rather than the term "device," the term "personal device" is utilized; this qualifying word presumably creates greater limitations on searches to an individual or entity's cell phone, tablet, or computer.[114] Senate Bill 2685 also focuses on the need to narrowly tailor searches by precluding the use of overly broad references to geographical location or communications service providers standing alone, which is omitted from House Bill 3361.[115]

The most notable difference between Senate Bill 2685 and House Bill 3361, in the section pertaining to PR and TT devices, is the specific inclusion of the stronger definition of "specific selection devices" and the definition of "address" as relating to physical and electronic addresses, such as an email, temporary network, or internet protocol address.[116]

As to FISA acquisitions for persons located outside of the United States, Senate Bill 2685 implicitly maintains standing minimization requirements, while House Bill 3361 specifically prohibits the dissemination of information stemming from persons located in the United States.[117] However, Senate Bill 2685 cites as applicable

---

111 *Compare* S. 2685 § 101(a), *with* H.R. 3361 § 101(a).

112 S. 2685 § 103(c) (amending section entitled "Prohibition on Bulk Collection of Tangible Things: Minimization Procedures").

113 *Compare* S. 2685 § 103(c), *with* H.R. 3361 Title I.

114 *Compare* S. 2685 § 107 (amending section entitled "Definitions"), *with* H.R. 3361 § 107 (as referred in the Senate).

115 *Compare* S. 2685 § 107 (amending section entitled "Definitions"), *with* H.R. 3361 § 107 (as referred in the Senate).

116 S. 2685 § 201 (amending section entitled "Prohibition on Bulk Collection").

117 *Compare* S. 2685 § 301 (amending section entitled "Limits on Use of Unlawfully Obtained Information"), *with* H.R. 3361 § 301 (amending section entitled "Clarification on Prohibition on Searching of Collections of Communications to Conduct Warrantless Searches for the Communications of United States Persons").

minimization procedures precluding the dissemination of non-public information regarding non-consenting United States person.[118]

Senate Bill 2685 also declines to create an Office of the Special Advocate, whose role would be to advocate for privacy issues.[119] However, like the passed version of House Bill 3361, it provides for *amici* to work with the FISC in analyzing applications and applying the law to same.[120] A further substantial difference is that Senate Bill 2685 requires the courts to appoint a panel of amici and provides explicit detail for their role in advocating before the court, including their ability to obtain independent technical experts to assist in their analysis of the issues.[121]

With regard to transparency in declassifying decisions, orders, and opinions of the FISC, Senate Bill 2685 and House Bill 3361 are identical, as outlined in the discussion of House Bill 3361, above.[122] Other transparency provisions have differing requirements, such as Senate Bill 2685's insistence that governmental reports be published on the Internet.[123] Senate Bill 2685 also requires greater specificity with respect to the information disclosed in such governmental reports, including the number of persons whose communications were collected and those who are believed to be located in the United States.[124] Likewise, Senate Bill 2685 provides slightly more specificity than House Bill 3361 relative to disclosures permitted by entities toward which FISC orders and national security letters are directed; other than the Senate provision prohibiting the disclosure of orders affecting new services or platforms for 540 days, the iterations are substantially similar.[125] Lastly, Senate Bill 2685 places

118 *See* 50 U.S.C. §§ 1801(h), 1821(4) (2012).

119 *Compare* S. 2685 § 401 (discussing the appointment of amicus curiae), *with* H.R. 3361 § 401 (as referred in the Senate) (establishing the Office of the Special Advocate).

120 *Compare* S. 2685 § 401 (discussing the appointment of amicus curiae), *with* H.R. 3361 § 401 (as referred in the Senate) (establishing the Office of the Special Advocate).

121 *Compare* S. 2685 § 401 (discussing the appointment of amicus curiae), *with* H.R. 3361 § 401 (as referred in the Senate) (establishing the Office of the Special Advocate).

122 *Compare* S. 2685 § 402 (amending section entitled "Declassification of Decisions, Orders, and Opinions"), *with* H.R. 3361 § 402 (as referred in the Senate) (amending section entitled "Foreign Intelligence Surveillance Court Disclosure of Opinions"), *and* S. 2685 § 101(a), *with* H.R. 3361 § 101(a).

123 S. 2685 §§ 602–03 (amending sections entitled "Annual Reports by the Government" and "Public Reporting by Persons Subject to FISA Orders," respectively).

124 *Compare* S. 2685 § 602 (amending section entitled "Annual Reports by the Government"), *with* H.R. 3361 § 603 (as referred in the Senate) (amending section entitled "Annual Reports by the Government on Orders Entered").

125 *Compare* S. 2685 § 603 (amending section entitled "Public Reporting by Persons Subject to FISA Orders"), *with* H.R. 3361 § 604 (as referred in the Senate) (amending section

limitations on the disclosure of national security letters if such would result in national security risks, interference with diplomatic relations, interference with investigations, or danger to the life and safety of any person.[126]

ii. Other Senate Bills

As in the House, several smaller bills have been introduced in the Senate, including the Ending Secret Law ("ESL") Act, the Surveillance Transparency Act ("STA"), the Freedoms and Privacy Act ("FPA"), and Senate Bill 1182, to amend FISA regarding evidence necessary to access business records.[127] Again, these bills occur in piecemeal rather than comprehensive fashion, but include some interesting provisions worth considering.

The ESL Act requires the disclosure of all FISC orders that involve interpretation of FISA subject to national security concerns, and if an order cannot be declassified under that basis, a summary of each decision must be released.[128] Senate Bill 1182 parallels the FREEDOM Act in setting forth stricter requirements by creating a factual basis upon which orders of production for documents and metadata can be sought.[129]

The STA seeks to expand government reporting requirements under NSA surveillance programs by requiring the Attorney General to submit an annual unclassified report that reflects: the total number of applications to the FISC for orders for production and for PR/TT use; the number of orders granted, modified, or denied; and good faith estimates for the number of individuals whose electronic information was collected through the NSA surveillance programs.[130] It also allows telecoms to issue biannual reports reflecting the number of orders received and complied with and the number of people whose information was collected pursuant to the orders.[131]

entitled "Public Reporting by Persons Subject to Orders").

[126] S. 2685 § 502 (amending section entitled "Limitations on Disclosure of National Security Letters").

[127] S. 1701, 113th Cong. § 1 (2013); S. 1452, 113th Cong. § 1 (2013); S. 1182, 113th Cong. § 1 (2013); S. 1130, 113th Cong. § 1 (2013).

[128] S. 1130 § 4 (amending section entitled "Requirement for Disclosure of Decisions, Orders, and Opinions of the Foreign Intelligence Surveillance Court").

[129] S. 1182 § 1 (amending section entitled "Specific Evidence for Court Orders to Produce Records and Other Items in Intelligence Investigations").

[130] S. 1452 § 2 (amending section entitled "Enhanced Public Reporting for Orders under the Foreign Intelligence Surveillance Act of 1978").

[131] *Id.* at § 3 (amending section entitled "Public Disclosures of Aggregate Information

The FPA amends FISA to allow individuals being federally prosecuted based on evidence garnered from NSA surveillance programs to seek discovery of the applications to, and orders for production or for PR and TT devices entered by, the FISC.[132] It also requires written certification by the Attorney General to use such evidence in criminal proceedings or to share the information within the law enforcement community and that these certifications must aggregate and summarize the incidences of utilizing the information in investigations or criminal proceedings in biannual reports to Congress.[133]

VI. STRENGTHS AND WEAKNESSES OF THE BILLS AND POTENTIAL RESOLUTIONS

It goes without saying that the standalone bills addressing only small portions of the NSA surveillance regime will not alone address the overreach concerns prevalent among the public, corporations, and Congress itself. Even taken together, they do not meet the level of institutional reform necessary to adequately address what is occurring. Senator Feinstein's proposal also does not sufficiently address concerns about the NSA's surveillance programs; rather, it appears to codify the NSA's ongoing activities, as it provides for additional oversight rather than reform as she believes that "[t]he NSA call-records program is legal and subject to extensive congressional and judicial oversight."[134]

As such, the USA FREEDOM Act stands alone as actually providing comprehensive reform, while also being politically palatable by allowing for possible bipartisan passage. Certainly, both the passed version of House Bill 3361 and the updated Senate Bill 2685 of the Act are not as strong as they were upon initial introduction, but they are still more comprehensive than the piecemeal bills. The more recent Senate version of Senate Bill 2685 is not a significantly far cry from the original iteration of the Act, save for the elimination of the Office of the Special Advocate, which could potentially create legal and constitutional issues.[135] Key improvements to the current regime include greater

Related to Orders Under the Foreign Intelligence Surveillance Act of 1978").

[132] S. 1701 § 2 (amending section entitled "Oversight and Disclosure Procedures of FISA Intelligence in Federal Proceedings").

[133] *Id.* at § 602 (amending section entitled "Reports to Congress on Intelligence Community and Law Enforcement Collaboration").

[134] *See* Sledge, *supra* note 103.

[135] *See* ANDREW NOLAN, RICHARD M. THOMPSON II, & VIVIAN CHU, CONG. RESEARCH SERV., R43260, REFORM OF THE FOREIGN INTELLIGENCE SURVEILLANCE COURTS:

transparency, through improved disclosure protocols that allow public acknowledgement of the number of orders for production entered against telecoms and the number of people affected, increased oversight by Congress through greater reporting requirements, and most importantly, creation of a process to allow for the appointment of amicus curiae who have expertise in privacy and civil liberties issues, intelligence collection, telecommunications, or other relevant fields to assist the FISC; all of which have generally received broad support.[136] The section providing for an Office of the Public Advocate has been removed from the House and Senate bills and replaced with the provision allowing for amicus curiae, potentially due to the constitutional and practical implications that maintaining a standing Special Advocate would entail.[137]

The FREEDOM Act is not without fault and could be strengthened by amending it to include some of the provisions of the piecemeal bills. For example, civil liberties advocates may feel that the FREEDOM Act does not strengthen minimization requirements to sufficiently address Judge Kollar-Kotelly's ruling that PR and TT devices need not require specific identification of the target, thus permitting dragnet collection of

INTRODUCING A PUBLIC ADVOCATE (Mar. 21, 2014) (The public advocate can potentially be viewed as an agent of the government and may act as a principal or inferior officer of the United States. The public advocate would be subject to the Article II Appointments Clause mandates. Under Article III, it is questionable whether such an advocate has standing to argue the "case" or "controversy" before the FISC due to the requirement that they have been injured, are threated to suffer injury by putatively illegal conduct, or are authorized to represent such an injured party. Likewise, Article III generally prohibits the government from litigating against itself, and allowing the advocate to seek relief on national security issues could invade core executive branch powers. Last, as the advocate would not be a party or representative of a party, they may not have standing to appeal FISC orders.); *see also* ANDREW NOLAN, RICHARD M. THOMPSON II, & VIVIAN CHU, CONG. RESEARCH SERV., OCT. 25, INTRODUCING A PUBLIC ADVOCATE INTO THE FOREIGN INTELLIGENCE SURVEILLANCE ACT'S COURTS: SELECT LEGAL ISSUES (2013); *cf.* Marty Lederman & Steve Vladick, *The Constitutionality of a FISA "Special Advocate,"* JUST SECURITY (Nov. 4, 2013, 1:34 PM), http://justsecurity.org/2873/fisa-special-advocate-constitution/ (arguing that Appointments Clause arguments may be rendered moot if the position were not permanent and the advocate was selected on a case-by-case basis, and even if they were a government employee, they would not exercise significant government authority, and thus not fall under Appointments Clause requirements. Likewise, the standing issue would be abrogated with properly drafted legislation by precluding the advocate from being a party to the case, but merely having a lawyer present, possibly for third parties whose metadata and communications are at issue. As to appeals, they propose legislation denoting the advocate in a role akin to a *guardian ad litem*, so that they could be representative of absent third parties).

136 *See generally* S. 2685, 113th Cong. (2014).

137 H.R. 3361, 113th Cong. § 401 (2014); S. 2685 § 401.

metadata.[138] This could be strengthened by including the portion of the SSR Act that requires a warrant for domestic surveillance.[139]

It is feasible that the FREEDOM Act could also incorporate some of Senator Feinstein's oversight provisions, such as allowing all members of Congress access to adequately redacted FISC orders.[140] However, there is still the issue of being able to provide full and adequate oversight of the program, without which runs the risk that the NSA could again run roughshod over Congress. The current system stymies oversight by only permitting members of Congress access to the classified information under which the NSA programs operate, disallowing them expert analysis of their own staffs and instead requiring reliance on the information provided by intelligence agencies in briefings, as the members do not have the time to review thousands of documents to make fully informed decisions on the subject.[141]

Even if the FISC transparency provisions permitting disclosure of orders are enacted, the FREEDOM Act still may not prove sufficient to allow for full and adequate congressional oversight. To that end, it would be worth considering creating a non-partisan Standing Joint Committee on Intelligence Oversight, akin to the Joint Committee on Taxation, that would be staffed by experts in national security and constitutional law issues. This committee staff would have the security clearance necessary to review the conduct of the NSA and any other involved agencies, outside of the auspices of the agency Inspectors General offices and the DOJ, so as to be able to provide clear guidance to Congress on the efficacy of reform and to ensure that the surveillance activities undertaken fall within constitutional confines and the enacted statutory regimes.[142]

---

[138] *See FISC Opinion*, *supra* note 32, at 23 ("The Court recognizes that by concluding that these definitions do not restrict the use of [PR] and [TT] devices to communication facilities associated with individual users, it is finding that these definitions encompass an exceptionally broad form of collection.").

[139] *See* H.R. 2818, 113th Cong. § 1 (2013).

[140] S. 1631, 113th Cong. § 5 (2013) (amending section entitled "Availability of Reports and Submissions").

[141] *See* Kessler, *supra* note 75 (describing that Rep. Ellison noted that the voluminous nature of the documents available required expert and staff assistance to review).

[142] It has been proposed that a Select Committee be established to investigate whether unconstitutional surveillance has occurred and whether officials acted improperly in doing so. However, this seems a temporary fix, which may dissolve into the realm of the political, rather than a long term option to adequately supervise this aspect of the intelligence community. *See* H. Res. 350, 113th Cong. § 3 (2013).

Other issues that the FREEDOM Act does not address include creating a cause of action for individuals and entities actually harmed by NSA surveillance and the appearance of NSA meddling in NIST encryption creation and gaining unauthorized access to overseas servers. The first issue will likely not be resolved for a variety of reasons, including that this would potentially make the government liable for an untold number of alleged Fourth Amendment infringements, and the real world eventuality that such liability would create an undue burden on the courts from the thousands of individual claims or class action claims that could seek to draw millions of citizens into the class that would immediately commence.

None of the proposed legislation addresses the issue of NSA/NIST collaboration in creating backdoors to encryption systems. Additional congressional oversight could address the issue, but to address it at the outset and staunch the financial harm befalling the United States tech industry, the most readily available way to address the issue, would be the budgetary mechanism of defunding the SIGINT Enabling Project. This would limit the NSA's ability to strong-arm NIST and major telecoms and reinstill public trust in the tech industry.[143]

Regardless of the potential for reform and transparency inherent in the FREEDOM Act, it still must overcome the major hurdle of being passed by both houses of Congress and signed into law by the President. Given the nature of the amendments made to the House passed version of the Act, it is unlikely that any Senate version of the bill will be strengthened by the provisions denoted above. Rather, even in its amended form, it may yet face roadblocks due to Senator Feinstein's competing bill, which received strong bipartisan support in the Intelligence Committee. Should the Senate pass the bill substantially unamended from its present form, it could still stall when returned to the House for passage or in Conference. As of September 2014, there were merely seven legislative calendar weeks left in the year, four of which are considered "lame duck" due to their occurrence after the mid-term elections.

[143] Nicole Gaouette, *NSA Spying Risks $35 Billion in U.S. Technology Sales*, BLOOMBERG (Nov. 26, 2013, 4:20 PM), http://www.bloomberg.com/news/2013-11-26/nsa-spying-risks-35-billion-in-u-s-technology-sales.html.

VII. PREEMPTIVE PRESIDENTIAL ACTION

An additional aspect of NSA surveillance reform that must be considered is the release of the Report and Recommendations of the President's Review Group on Intelligence and Communications Technology.[144] The Review Group issued a lengthy report stressing the need to maintain the public trust that has been damaged resulting from the Snowden disclosures and setting forth a list of forty-six reform recommendations.[145]

Many of these reform recommendations closely parallel the reform provisions set forth in the FREEDOM Act, including, but not limited to: requiring that the disclosure of metadata from third parties pursuant to FISC Order or National Security Letter be narrower in scope than currently provided for; permitting telecoms to release generic information pertaining to the number of orders received, complied with, and the scope of information produced; purging collected information on United States persons if collected through surveillance of foreign persons unless it has "foreign intelligence value or is necessary to prevent serious harm to others;" and creating the position of Public Interest Advocate to represent privacy and civil liberties interests before the FISC.[146] Other recommendations permit for the continued collection and storage of metadata by the telecoms themselves, or third parties, not the government, and for only limited government access to such information.[147] Still others would further limit executive power, already imperiled by the push toward bringing the administration and the NSA under greater congressional oversight, including making the Director of the National Security Agency subject to Senate confirmation, permitting that the Director be a civilian, and disallowing the Director from also being in charge of United States Cyber Command, a military unit.[148]

On January 17, 2014, the President announced that he would take efforts to implement reforms to foreign intelligence surveillance activities prior to March 28, 2014, the date of renewal for the law

144 RICHARD A. CLARK, ET AL., LIBERTY AND SECURITY IN A CHANGING WORLD: REPORT AND RECOMMENDATIONS BY THE PRESIDENT'S REVIEW GROUP ON INTELLIGENCE AND COMMUNICATIONS TECHNOLOGY (2013), *available at* http://www.nytimes.com/interactive/2013/12/19/us/politics/19nsa-review.html?_r=0 [hereinafter PRESIDENTIAL REPORT].

145 *Id.* at 17–18, 24–42.

146 *Id.* at 24, 28–29, 36 (discussing recommendations 1, 2, 12, 28).

147 *Id.* at 17.

148 *Id.* at 34, 210 (discussing recommendations 22–24).

authorizing metadata collection.[149] This includes three primary actions: decreasing the numbers of "hops" from a source phone number from which data can be collected; permitting that metadata be held by third parties rather than the government allowing access only through FISC approval; and creating the post of the public interest advocate.[150] A crucial aspect of these changes was the recommendation reducing the number of "hops" from a source phone number from three to two.[151] Procedural changes implemented include the requirement that the FISC approve queries of telephony metadata on a case-by-case basis and precluding the government from storing bulk metadata, placing the onus on the telephone companies to maintain the records only as they would in the ordinary course of business.[152] The public interest advocate position was not created, likely due to the constitutional and practical challenges to the implementation of such a position in such a short period of time, as outlined above.[153] Ultimately, the President's acts were limited in scope, and the amendments to the House's passed version of the USA FREEDOM Act align with the implemented changes in part.

VIII. CONCLUSION

To paraphrase the common understanding of Benjamin Franklin's quote, those who would give up an essential liberty for safety deserve neither liberty nor safety.[154] However, it seems we have already crossed

---

[149] Fred Kaplan, *Pretty Good Privacy: The Three Ambitious NSA Reforms Endorsed by Obama, and the One he Rejected*, SLATE (Jan. 17, 2014, 4:01 PM), http://www.slate.com/articles/news_and_politics/war_stories/2014/01/obama_s_nsa_reforms_the_president_s_proposals_for_metadata_and_the_fisa.html.

[150] *Id.* (A "hop" being a colloquial term indicating connections between phone numbers, i.e. one hop is the direct connection between the targeted phone number and all phone numbers it called, or received calls from. The second hop is the connection between the second tier of phone numbers and all phone number they called and received calls from. The third hop follows suit, bringing the potential amount of acquired metadata into the thousands or tens of thousands of phone numbers from a single target.).

[151] H.R Rep. No. 113–452, 14 (2014).

[152] *Id.*

[153] Ellen Nakashima, *Surveillance-court Judges Oppose White House Group's NSA Proposals*, WASH. POST (Jan. 14, 2014), http://www.washingtonpost.com/world/national-security/surveillance-court-judges-oppose-white-house-groups-nsa-proposals/2014/01/14/3c41e1e2-7d60-11e3-93c1-0e888170b723_story.html; *see* NOLAN ET AL., *supra* note 135.

[154] *See* Benjamin Wittes, *Would Benjamin Franklin Trade Liberty for Wiretapping?*, THE BROOKINGS INSTITUTE, (June 12, 2013 8:57 AM), http://www.brookings.edu/blogs/up-front/posts/2013/06/11-ben-franklin-liberty-wiretapping-security; *see also* Benjamin Wittes, *Against a Crude Balance: Platform Security and the Hostile Symbiosis Between Liberty and*

that Rubicon as a nation. The American public shares immeasurable amounts of information, both knowingly and unknowingly, with each other; corporations; and now the government, through our everyday acts on social media, online purchasing, and use of cell phones. We have reached a point where the public has few qualms with this proposition, save for the overreach of the government in collecting metadata on all communications, not including their content. Most Americans, too, are likely torn by the collections of communications metadata impinging on their privacy and the necessity to conduct global surveillance on increasingly tech savvy terrorist groups to prevent future attacks on American soil. This concern is highlighted by the discovery of westerners, including persons from the United States, attempting to join ranks with extremist groups, such as the Islamic State of Iraq and Syria.[155]

While it would be wonderful to return to the FISA scheme in place pre-9/11, that is no longer feasible from a technological, national security, sociopolitical, or even infrastructure-based standpoint, given current geopolitics, international terrorist threats, and the billions invested in surveillance and data storage infrastructure. As such, we appear to be relegated to imperfect reforms, the best of these being the USA FREEDOM legislation, which could still further be strengthened by amending it to include portions of the bills noted above and by creating a non-partisan joint committee within Congress, although the potential for the latter has not garnered much support.[156]

Although President Obama has taken action to reform the NSA's collection of domestic communication data, the FREEDOM Act should be enacted, regardless of any redundancies with administration policy. The Act will aid in providing greater transparency and oversight to the NSA surveillance programs currently in place and stem perceived violations of the Fourth Amendment.[157]

Security, THE BROOKINGS INSTITUTE (Sept. 21, 2011), *available at* http://www.brookings.edu/research/papers/2011/09/21-platform-security-wittes (the author argues that the quote is now routinely taken out of context and refers not to civil liberties, but to the "right of self-governance of a legislature in the interests of collective security").

[155] Michael S. Schmidt and Erick Schmitt, *U.S. Identifies Citizens Joining Rebels in Syria, Including ISIS*, N.Y. TIMES, Aug. 28, 2014, http://www.nytimes.com/2014/08/29/world/middleeast/us-identifies-citizens-joining-rebels-in-syria.html?_r=0.

[156] Representative Rokita's House Resolution 350 garnered only three cosponsors. H. Res. 350, 113th Cong. (2013).

[157] The USA FREEDOM Act, S. 2685, failed on a cloture vote by a vote of 58–42 in favor of cloture on November 18, 2014. The Library of Congress, *S. 2685 – USA FREEDOM*

Further, it has yet to be determined whether the mass collection of metadata actually violates the Fourth Amendment, given the opposite holdings of *Klayman* and *ACLU v. Clapper*. If the courts ultimately come down on the side of *Klayman* and civil libertarians, they may well follow Judge Leon's insight into evolving legal theory as it pertains to the Third Party Doctrine and *Smith v. Maryland*, as discussed above.

Since the Supreme Court, and no federal circuit court, has overturned *Smith*, Judge Leon's ruling that NSA surveillance violates the Fourth Amendment may not withstand initial appellate consideration on the basis of *stare decisis*. However, regardless of the outcome in the District of Columbia Circuit Court, the Supreme Court may well grant *certiorari*, and the Court will ultimately speak to the issue of whether mass NSA data collection is unconstitutional. Even absent taking up the *Klayman* case, the Court will, at a minimum, likely take up a similar issue in the context of whether there is a privacy expectation in protecting cell site location information generated when cell phones are used to prevent the government from being able access this information without a warrant due to a split between the circuit courts on the issue.[158]

To that end, the Court may help address these issues by adopting something akin to Professor Stephen Henderson's four-part test to determine whether Fourth Amendment privacy protections should apply to an individual, which, to a degree, coincides with the concerns expressed via the USA FREEDOM Act and the recommendations of the President's review panel. The test includes whether:

(1) The initial transfer of the information from the person to a third party is reasonably necessary to participate meaningfully in society or is socially beneficial, including to freedom of speech and association;

(2) The information is personal, including the extent to which it is intimate and likely to cause embarrassment or stigma if disclosed, and whether outside of the initial transfer to a third party it is typically disclosed only within one's close social network, if at all;

Act of 2014, CONGRESS.GOV. https://www.congress.gov/bill/113th-congress/senate-bill/2685?q={%22search%22%3A[%22\%22Usa+freedom\%22%22]} (last visited Dec. 29, 2014); U.S. SENATE, *U.S. Senate Roll Call Votes 113th Congress – 2nd Session*, http://www.senate.gov/legislative/LIS/roll_call_lists/roll_call_vote_cfm.cfm?congress=113&session=2&vote=00282 (last visited Dec. 29, 2014).

158 *See In re* United States for Historical Cell Site Data, 724 F.3d 600 (5th Cir. 2013) (holding that no warrants are required to obtain cell site data); *cf. In re* United States for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't, 620 F.3d 304 (3d Cir. 2010) (holding the government is required to show probable cause to obtain a warrant to gain access to cell site location information).

(3) The information is accessible to and accessed by nongovernment persons outside the institution; and

(4) Existing law restricts or allows access to and dissemination of the information or similar information.[159]

Until the courts begin addressing these privacy concerns, enactment of the FREEDOM Act will be a strong first step toward reform and transparency. However, if NSA overreach continues, there *may* be renewed and more vociferous calls to pursue the remedies suggested by Representative Holt, repealing the PATRIOT Act and the FISA Amendments Act, and starting anew.

Of course, this is neither practically nor politically feasible, and it must be questioned whether such would put the nation in a precarious national security scenario akin to that in place prior to 9/11, considering the growth of international terroristic activities. It is not a far reach to say that regardless of safeguards enacted by and oversight provided by Congress, as technological advances accelerate and now that the electronic surveillance infrastructure has been built, it will not be going away anytime soon. Accordingly, Congress and the American public must remain vigilant to strike a balance ensuring both that the nation's security is provided for and that the Fourth Amendment is not buried under the "need for security."

[159] Stephen E. Henderson, *The Timely Demise of the Fourth Amendment Third Party Doctrine*, 96 IOWA L. REV. BULL. 39, 50–51 (2011).