- Periodicals
  - Research Guides
  - OSU Libraries/WorldCat@OSU
  - Library Catalog
  - My Record
  - *Opinio Juris*
  - Moritz Legal Information Blog
  - Exam Archives
  - Audio/Visual Services
  - About the Moritz Law Library
  - New Acquisitions
- Programs & Centers
  - Alternative Dispute Resolution Program
  - Capstone Courses
  - Center for Interdisciplinary Law and Policy Studies
  - Democracy Studies
  - Distinguished Practitioners in Residence
  - Election Law @ Moritz
  - Externships
  - Justice for Children
  - Kirwan Institute for the Study of Race and Ethnicity
  - Law and Capital Markets
  - Master in the Study of Law (M.S.L.)
  - Master of Laws (LL.M.)
  - Mentoring and More @ Moritz
  - Moot Court Program
  - Oxford Study Abroad
  - Program on Law and Leadership
  - Service & Public Interest Programs
  - Washington, D.C. Summer Program
- Career Services
  - *for* Current Students
  - *for* Employers
  - *for* Alumni
  - *for* Prospective Students
  - Symplicity
  - Moritz Corporate Fellowship Program
- Clinics



## Online NSA Symposium

Below are preliminary working drafts of an articles to be included in a "paper symposium" to be published in *I/S: A Journal of Law and Policy for the Information Society* on 'NSA Surveillance: Issues of Security, Privacy, and Civil Liberty,' 9 ISJLP ___ (2014). The authors welcome reader comments:

### Upcoming Events

There are no upcoming events.

SEARCH OUR SITE

THE JOURNAL

**NSA Surveillance: Security, Privacy, and Civil Liberty**

Peter M. Shane, Foreword: The NSA and the Legal Regime for Foreign Intelligence Surveillance

**Debating Legality**

John Yoo, Foreword: The NSA and the Legal Regime for Foreign Intelligence Surveillance

Katherine Strandburg, Membership Lists, Metadata, and Freedom of Association's Specificity Requirement

Laura Donohue, PRISM and the Interception of Communications Under Section 702 of the Foreign Intelligence Surveillance Act

**Debating the Value of NSA Programs and of Their Secrecy**

Mark D. Young, National Insecurity: The Impacts of Illegal Disclosures of Classified Information

John Mueller and Mark G. Stewart, Secret without Reason and Costly without Accomplishment: Questioning the NSA's Metadata Program

**Assessing Civil Liberties Impacts**

Shayana Kadidal, NSA Surveillance: The Implications for Civil Liberties

Bryce Clayton Newell, The Massive Metadata Machine: Liberty, Power, and Secret Mass Surveillance in the U.S. and Europe

**Prospects for Change**

Nathan Alexander Sales, Domesticating Programmatic Surveillance: Some Thoughts on the NSA Controversy

Stephen I. Vladeck, Standing and Secret Surveillance

Reed E. Hundt, Making No Secrets About It

**Keynote Essay**

Amitai Etzioni, A Cyber Age Privacy Doctrine: A Liberal Communitarian Approach

I/S: A Journal of Law and Policy for the Information Society is an interdisciplinary journal of research and commentary concentrating on the intersection of law, policy, and information technology. I/S represents a one-of-a-kind partnership between one of America's leading law schools, the Moritz College of Law at The Ohio State University, and the nation's foremost public policy school focused on information technology, Carnegie Mellon University's Heinz College.

Preliminary Draft 2.5 – Please Do Not Cite Without Permission
To be Published in *I/S: A Journal of Law and Policy for the Information Society*
9 ISJLP ___ (2014).
http://www.is-journal.org

# FOREWORD: THE NSA AND THE LEGAL REGIME FOR FOREIGN INTELLIGENCE SURVEILLANCE

Peter M. Shane[1]

"Mr. President, no one is saying you broke any laws, we're just saying it's a little bit weird you didn't have to."

- John Oliver[2]

As the papers in this symposium demonstrate, serious commentators reviewing the National Security Agency (NSA) surveillance programs that have been revealed through recent leaks are far from unanimous that the programs are lawful.[3] The point of John Oliver's joke, however, still rings true: Somehow, our laws have evolved to a stage where lawyers could plausibly defend the government's entitlement to capture and store an immense volume of our telephone and online communications, as well as metadata about both. For many Americans, this is a breathtaking reality. The point of this Article is to explain our legal evolution as a way of providing context for the *I/S* symposium on "NSA Surveillance: Security, Privacy, and Civil Liberty." It will introduce the papers that follow, and offer some concluding thoughts on the issues of executive power that lurk behind the controversy.

## 1. Intercepting Communication Contents: From *Olmstead* to the Foreign Intelligence Surveillance Act

[1] Jacob E. Davis and Jacob E. Davis II Chair in Law, Moritz College of Law, Ohio State University.

[2] The Daily Show, June 10, 2013, available at http://www.thedailyshow.com/watch/mon-june-10-2013/the-daily-show-with-john-oliver.

[3] Compare John Yoo, *The Legality of the National Security Agency's Bulk Data Surveillance Programs*, 9 ISJLP ___ (2014) (defending NSA surveillance), *with* Katherine Strandburg, *Membership Lists, Metadata, and Freedom of Association's Specificity Requirement*, 9 ISJLP ___ (2014) (challenging NSA metadata collection under the First Amendment) and Laura Donohue, *PRISM and the Interception of Communications Under Section 702 of the Foreign Intelligence Surveillance Act*, 9 ISJLP ___ (2014) (challenging NSA's current programs of electronic surveillance under the Fourth Amendment). On possible statutory challenges to the legality of the metadata collection programs, see text at notes ---, *infra*.

Prior to the late 1960s, the federal government did not interpret law as constraining its entitlement to collect the contents of communications through electronic surveillance for either criminal investigation or national security purposes. The Supreme Court had held in 1928 that a wiretap was not a Fourth Amendment "search," because it involved neither physical trespass, nor the seizure of a tangible thing.[4] Three years later, Attorney General William D. Mitchell issued the first authorization for telephone wiretapping, then aimed at syndicated bootleggers.[5]

In 1934, Congress enacted a legal ban on wiretaps, providing in the Federal Communications Act that it would be a felony for any person "to intercept and divulge or publish the contents of wire and radio communications."[7] Although the Supreme Court held the prohibition applicable to federal agents[6] – thus rendering wiretap evidence inadmissible at trial – the Justice Department interpreted the law and the Court's decisions as forbidding only the public divulgence of intercepted communications, not wiretapping itself.[7] As a result, when President Roosevelt informed the Attorney General in 1940 of his view that counterintelligence wiretaps were constitutional, the Justice Department did not perceive any Fourth Amendment bar to their use for national security purposes.[8]

The government expanded its use of national security wiretaps from the Roosevelt through the Nixon Administrations. The Truman Administration even abandoned the Roosevelt policy of limiting its targets "insofar as possible" to aliens.[9] The Eisenhower Administration took the position that surreptitious physical entry to conduct wiretapping was likewise legally

---

4 Olmstead v. United States, 277 U.S. 468 (1928).

5 Foreign Intelligence Surveillance Act of 1978, H. Rept. No. 95-1283, Pt. I, 95th Cong., 2d Sess. 15 (1978) (hereafter, "House FISA Report").

7 47 U.S.C. § 605.

6 Nardone v. United States, 302 U.S. 379 (1937); 308 U.S. 338 (1939).

7 House FISA Report, *supra* note 5, at 15.

8 Id.

9 Id., at 16.

authorized.[10] As recounted in a House report: "From the relatively limited authorization of warrantless electronic surveillance under President Roosevelt, . . . the mandate for the FBI was quickly expanded to the point where the only criterion was the FBI's subjective judgment that the 'national interest' required the electronic surveillance."[11]

With two critical decisions, however, the Supreme Court radically changed the relevant legal landscape. The Court's 1967 decision in *Katz v. United States*[12] overruled *Olmstead* and applied the Fourth Amendment's warrant provision to electronic surveillance in connection with a criminal prosecution. Congress responded by enacting Title III of the Omnibus Crime Control and Safe Streets Act of 1968,[13] providing standards to govern, and a process for obtaining, criminal wiretap warrants. The Act explicitly provided, however, that it worked no change in the President's authority to engage in surveillance "to obtain foreign intelligence information deemed essential to the security of the United States, or to protect national security information against foreign intelligence activities."[14]

Notwithstanding this disclaimer, the Supreme Court proceeded to decide, in the 1976 *Keith* case,[15] that warrantless surveillance was also unconstitutional in the context of wholly domestic national security investigations. At least where "[t]here is no evidence of any involvement, directly or indirectly, of a foreign power,"[16] the Court found no categorical exception to the warrant requirement. In balancing the competing values at stake, the Court

---

10 Id.
11 Id.
12 389 U.S. 347 (1967).
13 Pub. L. 90–351, Title III, 82 Stat. 212 (1968), codified as amended, 18 U.S.C. §§ 2510-2520 (2012).
14 Pub. L. 90–351, § 802, 82 Stat. 213 (1968), codified at 18 U.S.C. § 2511(3).
15 United States v. United States District Court (Keith), 407 U.S. 297 (1972). The case is commonly known by the name of the U.S. District Court Judge whose order was under review.
16 Id., at 309.

observed: "Though the investigative duty of the executive may be stronger in [national security] cases, so also is there greater jeopardy to constitutionally protected speech."[17]

The *Keith* Court went beyond its Fourth Amendment holding to opine that the requirement of prior magistrate approval for national security warrants did not demand that such warrants be issued only on grounds identical to Title III criminal prosecution warrants.[18] The Court expressly invited Congress to tackle the problem, stating: "Different standards may be compatible with the Fourth Amendment if they are reasonable both in relation to the legitimate need of Government for intelligence information and the protected rights of our citizens."[19]

Congress's acceptance of the Court's invitation, however, was colored by revelations in 1975 and 1976 that the CIA, FBI, and other intelligence-gathering units within the executive branch had engaged in massive, illegal domestic intelligence operations during the Nixon administration.[20] Reports of CIA abuse led President Ford to name an eight-member commission (including future President Reagan) under Vice President Rockefeller to investigate alleged CIA statutory violations.[21] On January 15, 1975, CIA Director William Colby presented a lengthy report to the Senate Appropriations Intelligence Operations Subcommittee, acknowledging that the CIA had carried out surveillance of journalists and political activists, opened the mail of U.S. citizens, infiltrated domestic protest groups and gathered information for

---

17 Id., at 313.

18 Id., at 322.

19 Id.

20 Final Report of the Select Committee to Study Governmental Operations with Respect to Intelligence Activities – Book 2: Intelligence Activities and the Rights of Americans, S. Rept. No. 94-755, 94th Cong., 2d Sess. 1-20 and passim (1976); see generally Final Report of the Select Committee to Study Governmental Operations with Respect to Intelligence Activities – Book 3: Supplementary Detailed Staff Reports on Intelligence Activities and the Rights of Americans, S. Rept. No. 94-755, 94th Cong., 2d Sess. (1976).

21 Report to the President by the Commission on CIA Activities within the United States, at ix (1975).

secret files on more than 10,000 Americans.[22] Twelve days later, the Senate established an eleven-member select committee under Senator Frank Church ("Church Committee") to investigate the activities of the CIA, FBI, and other law enforcement and intelligence agencies to determine if they had engaged in any illegal or unethical intelligence activities during the Vietnam period.[23] (A parallel study was later undertaken in the House of Representatives, under Rep. Otis G. Pike, of New York.)[24]

What followed in the wake of *Keith* and the Church Committee report was an intense interbranch collaboration between Congress and, first, the Ford Administration, later the Carter Administration, on the drafting of what became the Foreign Intelligence Surveillance Act of 1978 (FISA).[25] FISA was enacted on Congress's understanding, in which Attorneys General Levi and Bell concurred, that "Congress has at least concurrent authority to enable it to legislate with regard to the foreign intelligence activities of departments and agencies of this Government either created or funded by Congress."[26] As described in a House committee report, Congress's "presumption" in designing FISA was that "whenever an electronic surveillance for foreign intelligence purposes may involve the fourth amendment rights of any U.S. person, approval for such a surveillance should come from a neutral and impartial magistrate."[27]

Even in its original form, FISA was a dauntingly complex statute. It created an entirely new and unprecedented institution – the Foreign Intelligence Surveillance Court (FISC) – to

---

[22] Senate Committee on Intelligence Activities: Report of the Committee on Government Operations to Accompany S. Res. 400 Resolution to Establish a Standing Committee of the Senate on Intelligence Activities, And For Other Purposes, S. Rept. No. 94-675, 94th Cong., 2d Sess. 4 (1976).

[23] Final Report of the Select Committee to Study Governmental Operations with Respect to Intelligence Activities – Book 1: Foreign and Military Intelligence, S. Rept. No. 94-755, 94th Cong., 2d Sess. 2-3 (1976).

[24] Gerald K. Haines, *The Pike Committee Investigations and the CIA: Looking for a Rogue Elephant*, CSI STUDIES IN INTELLIGENCE 81-92 (Winter 1998-99), available at https://www.cia.gov/library/center-for-the-study-of-intelligence/kent-csi/vol42no5/pdf/v42i5a07p.pdf.

[25] Pub.L. 95–511, 92 Stat. 1783 (1978); House FISA Report, *supra* note 5, at 13-14.

[26] Id., at 24.

[27] Id., at 24-25.

superintend the process of authorizing foreign intelligence surveillance.[28] The FISC's membership, designated by the Chief Justice of the United States, comprises 11 district court judges who must represent at least seven of the United States judicial circuits. In addition, the Chief Justice designates three judges – from either the district courts or courts of appeals – to constitute a review panel to which the United States may appeal any FISC decision denying a warrant application. The court's novelty, other than in its membership and selection, lay in its secrecy. Its proceedings are entirely ex parte; should the Government petition for certiorari review of any decision adverse to the Government that is upheld on appeal, what is now called the FISC Court of Review transmits the record of the matter to the Supreme Court under seal.[29]

Hidden in FISA's definitional sections, as well as its operative provisions, were a host of important policy decisions regarding the scope of permissible surveillance. One was to permit the Attorney General to authorize warrantless foreign intelligence surveillance, for a year at a time, where directed exclusively at communications between foreign powers;[30] conversely, no authority was provided at all under FISA for national security investigations that lacked any international or foreign dimension. As a result, electronic surveillance directed at a wholly domestic national security threat, as in *Keith*, must still be authorized under the Title III probable cause standard.

For electronic surveillance directed at foreign intelligence, however – assuming it is not exclusively between "foreign powers" as defined in the Act – FISA makes a critical concession to the executive branch in relaxing the standard for a surveillance warrant. Specifically, it is not necessary, as with a Title III warrant, that probable cause exist to believe the surveillance will yield evidence of a crime; in applying for a FISA warrant, the Attorney General has to certify

---

28 Pub. L. 95–511, § 103, 92 Stat. 1788 (1978), codified at 50 U.S.C. § 1803.

29 Id., at § 1803(b).

30 Pub. L. 95–511, § 102, 92 Stat. 1786 (1978), codified at 50 U.S.C. § 1802(a)(1).

instead that "the purpose of the surveillance is to obtain foreign intelligence information" and the official certifying the warrant application to the Foreign Intelligence Surveillance Court "deems the information sought to be foreign intelligence information."[31]

The character of the information sought, however, is not sufficient by itself to sustain a FISA warrant application. A FISA warrant – and thus the relaxation of the probable cause standard – is available to the government only if "the target of the electronic surveillance is a foreign power or an agent of a foreign power."[32] "United States persons" – essentially, citizens and lawfully resident aliens – cannot literally be "foreign powers," although surveillance directed a foreign power may cover such persons if they belong to a faction of a foreign nation or nations, a group engaged in or preparing for international terrorism, or a foreign-based political organization.[33] Americans may also be targeted for surveillance if they are "agents of a foreign power." This would include persons who knowingly aid and abet acts in preparation for international terrorism.[34]

---

[31] Pub. L. 95–511, § 104, 92 Stat. 1788 (1978), codified at 50 U.S.C. § 1804(a)(6)(A) and (B). The USA PATRIOT Act, Pub. L. 107–56, § 218, 115 Stat. 291 (2001) changed "the purpose" in 50 U.S.C. § 1804(a)(6)(B) to "a significant purpose."

FISA originally defined "foreign intelligence information," as follows:

(1) information that relates to, and if concerning a United States person is necessary to, the ability of the United States to protect against--,

(A) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power;

(B) sabotage or international terrorism by a foreign power or an agent of a foreign power; or

(C) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power; or

(2) information with respect to a foreign power or foreign territory that relates to, and if concerning a United States person is necessary to--,

(A) the national defense or the security of the United States; or

(B) the conduct of the foreign affairs of the United States.

Pub. L. 95–511, § 101, 92 Stat. 1783 (1978), codified as amended at 50 U.S.C. § 1801(e) (1982). In 2008, "sabotage or international terrorism" in subparagraph (1)(B) was deleted and "sabotage, international terrorism, or the international proliferation of weapons of mass destruction" inserted in its place. Pub. L. 110–261, § 110(a), 122 Stat. 2465 (2008).

[32] Pub. L. 95–511, § 104(a)(3)(A), 92 Stat. 1788 (1978), codified as amended at 50 USC § 1804(a)(3)(A).

[33] Pub. L. 95–511, § 101(a), 92 Stat. 1783, codified as amended at 50 U.S.C. § 1801(a).

[34] "Agent of a foreign power" means--

(1) any person other than a United States person, who--

But perhaps FISA's most obscure policy choices are embedded in its definition of "electronic surveillance."[35] The definition of "electronic surveillance" was written to cover several categories of information acquisition by "an electronic, mechanical, or other surveillance device." Such a device is covered categorically if used to intercept "any wire communication to or from a person in the United States, without the consent of any party thereto, if such acquisition occurs in the United States."[36] If used to intercept the contents of any radio communication, such a device is covered if the interception was intentional and "under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes, and if both the sender and all intended recipients are located within the United States."[37] With regard to both wire and radio communications, interception is covered with regard to any "communication sent by or intended to be received by a particular, known United States person who is in the United States, if the contents are acquired by intentionally targeting that United States person, under circumstances in which a person has a

---

(A) acts in the United States as an officer or employee of a foreign power, or as a member of a foreign power as defined in subsection (a) (4);

(B) acts for or on behalf of a foreign power which engages in clandestine intelligence activities in the United States contrary to the interests of the United States, when the circumstances of such person's presence in the United States indicate that such person may engage in such activities in the United States, or when such person knowingly aids or abets any person in the conduct of such activities or knowingly conspires with any person to engage in such activities; or

(2) any person who--,

(A) knowingly engages in clandestine intelligence gathering activities for or on behalf of a foreign power, which activities involve or may involve a violation of the criminal statues of the United States;

(B) pursuant to the direction of an intelligence service or network of a foreign power, knowingly engages in any other clandestine intelligence activities for or on behalf of such foreign power, which activities involve or are about to involve a violation of the criminal statutes of the United States;

(C) knowingly engages in sabotage or international terrorism, or activities that are in preparation therefor, for or on behalf of a foreign power; or

(D) knowingly aids or abets any person in the conduct of activities described in subparagraph (A), (B), or (C) or knowingly conspires with any person to engage in activities described in subparagraph (A), (B), or (C).

Pub. L. 95–511, § 101(b), 92 Stat. 1783, codified as amended at 50 U.S.C. § 1801(b).

[35] Pub. L. 95–511, § 101(f), 92 Stat. 1783, codified as amended at 50 U.S.C. § 1801(f).

[36] Id., at § 101(f)(2), 92 Stat. 1783, codified as amended at 50 U.S.C. § 1801(f)(2).

[37] Id., at § 101(f)(3), 92 Stat. 1783, codified as amended at 50 U.S.C. § 1801(f)(3).

reasonable expectation of privacy and a warrant would be required for law enforcement purposes."[38]

What these definition may well obscure for the uninitiated reader are the categories of what is, in fact, electronic surveillance, but that FISA apparently permits to proceed without warrants. Most notably, communications wholly outside the United States are exempt, no matter who participates. Also, acquisitions of radio (i.e., wireless) communications are not covered unless they occur "under circumstances in which a person has a reasonable expectation of privacy," circumstances that legislators expected would not cover, for example, citizens band or ham radio transmissions.[39]

What also may not be obvious is that Congress understood the coverage for "the *contents* of any wire communication to or from a person in the United States" to include what is now commonly called metadata, i.e., information identifying the calling and receiving devices involved in a communication and indicating the length of that communication. In identical language, the relevant committee reports stated:

> The surveillance covered by subparagraph (B) is not limited to the acquisition of the oral, or verbal contents of a wire communication. It includes the acquisition of any other contents of the communication, for example, where computerized data is transmitted by wire. Therefore, it includes any form of "pen register" or "touch-tone decoder" device which is used to acquire, from the contents of a wire communication, the identities or locations of the parties to the communication.[40]

---

[38] Id., at § 101(f)(1), 92 Stat. 1783, codified as amended at 50 U.S.C. § 1801(f)(1). The fourth definition encompasses "the installation or use of an electronic, mechanical, or other surveillance device in the United States for monitoring to acquire information, other than from a wire or radio communication, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes." Id., at § 101(f)(4), 92 Stat. 1783, codified as amended at 50 U.S.C. § 1801(f)(4).

[39] House FISA Report, *supra* note 5, at 52.

[40] House FISA Report, *supra* note 5, at 51; Foreign Intelligence Surveillance Act of 1978, S. Rept. No. 95-701, 95th Cong., 2d Sess. 35 (1978).

Because the legislative history as well as the statutory language of FISA was the subject of intense interbranch negotiation, it is reasonable to expect that the Justice Department subsequently interpreted FISA to permit pen register warrants as well.

**2. Bulk Information, ECPA and the USA PATRIOT Act**

The devices that capture information about communications one initiates are called "pen registers."[41] Devices that capture such information about communications people receive are called "trap and trace" devices.[42] Despite FISA's tacit reference to "electronic devices" used to capture information about communications apart from their actual contents, it was not until eight years later that Congress regulated the use of such devices comprehensively. Congress regulated both pen registers and trap and trace devices under the Electronic Communications Privacy Act of 1986 (ECPA), which prohibited the use of such devices except pursuant to either a FISA warrant or ECPA itself. [43] Notably, however, the standard for obtaining a pen register warrant under ECPA is arguably even less demanding than the FISA standard. The applicant agency for such a warrant need only certify "that the information likely to be obtained is relevant to an ongoing criminal investigation being conducted by that agency."[44]

---

[41] Under the Electronic Privacy Communication Act, "the term 'pen register' means a device or process which records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, provided, however, that such information shall not include the contents of any communication, but such term does not include any device or process used by a provider or customer of a wire or electronic communication service for billing, or recording as an incident to billing, for communications services provided by such provider or any device or process used by a provider or customer of a wire communication service for cost accounting or other like purposes in the ordinary course of its business." Pub. L. No. 99–508, § 301(a), 100 Stat. 1870 (1986), codified as amended at 18 U.S.C. § 3127(3). (Provisions of the ECPA that, as of 1986, were codified at 18 U.S.C. §§ 3125-3126 were renumbered §§ 3126-3127 with the addition of a new § 3125 in 1988. Pub. L. 100–690, § 7092(a)(2), 102 Stat. 4410 (1988).)

[42] Under the Electronic Communications Privacy Act, "the term 'trap and trace device' means a device or process which captures the incoming electronic or other impulses which identify the originating number or other dialing, routing, addressing, and signaling information reasonably likely to identify the source of a wire or electronic communication, provided, however, that such information shall not include the contents of any communication." Id., codified as amended at 18 U.S.C. § 3127(4).

[43] Pub. L. No. 99–508, § 301(a), 100 Stat. 1870 (1986), codified as amended at 18 U.S.C. §§ 3121(a).

[44] Id., at 100 Stat. 1869, codified as amended at 18 U.S.C. §§ 3122(b)(1).

In 1998, Congress made explicit that FISA authorized pen register warrants and expanded the scope of that authority. Under Section 601 of the Intelligence Authorization Act for Fiscal Year 1999, the government may get such a device based on:

> information which demonstrates that there is reason to believe that the telephone line to which the pen register or trap and trace device is to be attached, or the communication instrument or device to be covered by the pen register or trap and trace device, has been or is about to be used in communication with—
>
> (A) an individual who is engaging or has engaged in international terrorism or clandestine intelligence activities that involve or may involve a violation of the criminal laws of the United States; or
>
> (B) a foreign power or agent of a foreign power under circumstances giving reason to believe that the communication concerns or concerned international terrorism or clandestine intelligence activities that involve or may involve a violation of the criminal laws of the United States.[45]

The apparent basis, however, for much of the NSA's bulk collection of metadata arises under the so-called USA PATRIOT Act.[46] That statute, which substantially amended a dozen other laws regulating the government's investigative authorities, was enacted under intense executive branch pressure in the immediate wake of 9/11. In contrast to the extensive interbranch negotiation and painstaking documentation that accompanied FISA, Congress enacted the PATRIOT Act less than two months after the September 11 attacks and without carefully crafted analysis to guide its implementation.[47]

---

[45] Pub. L. No. 105–272, 112 Stat. 2396, 2405 (1998). The USA PATRIOT ACT, Pub. L. 107–56, § 214(a), 115 Stat. 286 (2001), deleted this language and substantially rewrote the FISA provisions on pen registers and trap and trace devices. The current requirement is only that "the information likely to be obtained is foreign intelligence information not concerning a United States person or is relevant to an ongoing 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." 50 U.S.C. § 1842(c)(2).

[46] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, Pub. L. 107–56, 115 Stat. 271 (2001) (hereafter, the "USA PATRIOT Act" or "PATRIOT Act").

[47] "Legislative proposals in response to the terrorist attacks of September 11, 2001 were introduced less than a week after the attacks. President Bush signed the final bill, the USA PATRIOT Act, into law on October 26, 2001. Though the Act made significant amendments to over 15 important statutes, it was introduced with great haste and passed with little debate, and without a House, Senate, or conference report. As a result, it lacks background

Among the key changes that expanded the government's information gathering authority were an expansion of the definitions of "pen register" and "trap and trace" devices. ECPA previously authorized their use for telephone communications.[48] They are now defined to permit surveillance of routing information for all electronic communications, including, for example, Web surfing and email.[49]

Pen register authority was also extended so that its target need no longer be a foreign power or the agent of a foreign power. Under Section 214 of the Act, FISA was amended so that a pen register or trap and trace device may be sought in connection with any investigation "to protect against international terrorism or clandestine intelligence activities."[50] The only limitation regarding the use of such devices targeting United States citizens is that "such

---

legislative history that often retrospectively provides necessary statutory interpretation." Electronic Privacy Information Center, *USA PATRIOT Act*, EPIC.ORG, available at http://epic.org/privacy/terrorism/usapatriot/.

[48] Pub. L. No. 99–508, § 301(a), 100 Stat. 1871 (1986).

[49] Pub. L. 107–56, § 216(c)(2) and (3), 115 Stat. 290 (2001), codified at 18 U.S.C. § 3127. Expanding the government's authority through a mere definitional change, however, built into the law a potentially important ambiguity. Under ECPA, neither kind of device is to be used to observe "the contents of any communication." 18 U.S.C. § 3121(c). The distinction between content and routing information is readily implemented with regard to telephone communications. That distinction is far less obvious, however, for email. That is because email communications move across a variety of conduits that use routing information of different kinds. To oversimplify, an Internet Service Provider (ISP) needs only two pieces of information to route an electronic message – the IP address of the sending device and the address of the recipient server, which may belong, say, to Google, Yahoo!, or the like. The ISP does not need to consult the "header" information that indicates, for example, the actual intended recipient of the email. As far as the ISP is concerned, the "header" is content. For Google, however, the header is routing information. Google has to get its Gmail to the correct individual subscriber. Julian Sanchez, *Are Internet Backbone Pen Registers Constitutional?*, JUSTSECURITY.ORG (Sept. 23, 2013), available at http://justsecurity.org/2013/09/23/internet-backbone-pen-registers-constitutional/. In any event, we now know from redacted FISC opinions declassified and released by the Office of the Director of National Intelligence that the FISC had to wrestle seriously with the distinction between "content," the collection of which is not permitted through pen register or trap and trace orders, and "dialing, routing, addressing, or signaling information," which is permissible. See Undated Opinion by Judge John D. Bates Declassified Without Date or Caption (FISC), at 30-35, 52-54, available at http://www.dni.gov/files/documents/1118/CLEANEDPRTT%202.pdf (approving the re-initiation of pen register and trap and trace authority under FISA for Internet metadata). Although the opinion redacts all specifics about the precise categories of information NSA proposes to collect as metadata, we know from another declassified opinion that "information from the 'from' line of an email" is included. Undated Opinion by Judge Colleen Kollar-Kotelly Declassified Without Date or Caption (FISC), at 15, available at http://www.dni.gov/files/documents/1118/CLEANEDPRTT%201.pdf.

[50] The USA PATRIOT ACT, Pub. L. 107–56, § 214(a), 115 Stat. 286 (2001), codified at 50 U.S.C. § 1842(c)(2).

investigation of a United States person" may not be "conducted solely upon the basis of activities protected by the first amendment to the Constitution."[51]

Arguably, the most consequential change, however, appears to be the enactment of Section 215 of the Act, which authorizes the FBI Director or a designee to seek:

> an order requiring the production of any tangible things (including books, records, papers, documents, and other items) 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.[52]

The application for such authority need only "specify that the records concerned are sought for an authorized investigation . . . to protect against international terrorism or clandestine intelligence activities."[53] As it turns out, the Bush and Obama Administrations have relied on Section 215 to acquire telephone company records of the metadata concerning millions and millions of phone calls.[54] Because this acquisition does not entail the government's use of an electronic surveillance device, FISA does not apply.

### 3. The 2005 NSA Leaks

As expansive as these authorities may seem, it was revealed in a series of New York Times articles in 2005 that the Bush Administration, since shortly after 9/11, had been engaged in extensive warrantless wiretapping outside the FISA process.[55] The Times also revealed in

---

[51] Id.

[52] Pub. L. 107–56, § 215, 115 Stat. 287 (2001), codified as amended at 50 U.S.C. § 1861(a).

[53] Id., codified as amended at 50 U.S.C. § 1861(b)(2).

[54] Glenn Greenwald, *NSA collecting phone records of millions of Verizon customers daily*, THE GUARDIAN (June 5, 2013), available at http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order.

[55] James Risen and Eric Lichtblau, *Bush Lets U.S. Spy on Callers Without Courts*, N.Y. Times (Dec. 16, 2005), available at http://www.nytimes.com/2005/12/16/politics/16program.html?pagewanted=all&_r=0; Eric Lichtblau and James Risen, *Eavesdropping Effort Began Soon After Sept. 11 Attacks*, N.Y. TIMES (Dec. 18, 2005), available at http://query.nytimes.com/gst/fullpage.html?res=F70716F73D540C7B8DDDAB0994DD404482; James Risen and Eric Lichtblau, *Spying Program Snared U.S. Calls*, N.Y. Times (Dec. 21, 2005), available at http://www.nytimes.com/2005/12/21/politics/21nsa.html.

general terms the existence of a broad data mining program.[56] Unlike the 1975 New York Times revelations of unlawful surveillance during the 1960s, however, the 2005 revelations prompted no comprehensive public inquiry or any establishment of a clear historical record of what happened, why, and with whose approval. It is important to take note of what we now transpired because the further 2006 amendments to the PATRIOT Act[57] and the amendments to FISA that occurred in 2007[58] and 2008[59] were intended precisely to make lawful much of what had been of dubious legality, at best, under the Bush Administration.

The clearest, albeit still incomplete record of what we now know concerning Bush Administration surveillance and the decision making surrounding that surveillance comes from two documents. One is an "Unclassified Report on the President's Surveillance Program" released on July 10, 2009,[60] which was jointly prepared, as required by the FISA Amendments Act of 1978,[61] by the Inspectors General of Justice, Defense, the CIA, the NSA, and the Office of the Director of National Intelligence. The second is a draft March 24, 2009 report by the NSA Office of Inspector General that was leaked by Edward Snowden.[62] Events are perhaps easiest to follow if traced with regard to particular categories of communications that NSA sought to intercept: first, the contents of telephone and Internet communications; second, telephone metadata; and third, Internet metadata. All were part of what the IG Report calls the "President's

---

56 Eric Lichtblau and James Risen, *Spy Agency Mined Vast Data Trove, Officials Report*, N.Y. Times (Dec. 24, 2005), available at http://www.nytimes.com/2005/12/24/politics/24spy.html?pagewanted=all&_r=0.

57 See text at notes ___, *infra*.

58 See text at notes ___, *infra*.

59 See text at notes ___, *infra*.

60 Unclassified Report on the President's Surveillance Program (July 10, 2009), available at https://www.fas.org/irp/eprint/psp.pdf (hereafter, "2009 Unclassified PSP Report").

61 FISA Amendments Act of 2008, Pub. L. No. 110-261, § 301(c), 122 Stat. 2472 (2008).

62 Office of the Inspector General, National Security Agency Central Security Service, ST-09-0002 Working Draft (March 24, 2009), available at http://www.aclu.org/files/natsec/nsa/20130816/NSA%20IG%20Report.pdf (hereafter, "NSA IG Report").

Surveillance Program" (PSP), which includes, but goes significantly beyond the Terrorist Surveillance Program revealed in the 2005 New York Times stories.

September 11, for obvious reasons, prompted NSA's interest in substantially expanding its acquisition of telephony and Internet content that might reveal foreign intelligence information. Thus, on September 14, 2001, NSA Director General Michael Hayden "approved the targeting of terrorist-associated foreign telephone numbers on communication links between the United States and foreign countries where terrorists were known to be operating."[63] At first, calls originating in the United States were collected only if communicating with specified, pre-approved numbers, but this net was expanded.[64] By September 26, General Hayden had determined that any Afghan telephone number in contact with a U.S. telephone number "was presumed to be of foreign intelligence value and could be disseminated to the FBI."[65]

During this period, General Hayden was apparently in discussions with CIA Director George Tenet and the White House about the feared inadequacy of existing legal authorities to permit the kinds of expanded acquisition that could be useful in the wake of September 11.[66] As a consequence, President Bush, on October 4, 2011, issued a secret memorandum entitled, "Authorization for Specified Electronic Surveillance Activities During a Limited Period to Detect and Prevent Acts of Terrorism Within the United States."[67] As summarized in the Draft NSA IG Report, under the President's order:

> NSA could collect the content and associated metadata of telephony and Internet communications for which there was probable cause to believe that one of the communicants was in Afghanistan or that one communicant was engaged in or preparing for acts of international terrorism. In addition, NSA was authorized to acquire telephony and Internet metadata for communications with at least one

63 Id., at 3.
64 Id.
65 Id.
66 Id., at 4, 6-7.
67 Id., at 1.

> communicant outside the United States or for which no communicant was known to be a citizen of the United States. NSA was also allowed to retain, process, analyze and disseminate intelligence from the communications acquired under the authority.[68]

This authorization was subsequently modified from time-to-time depending, one presumes, on the White House's assessment of the scope of national security needs.[69]

With regard to both telephony and Internet content, the acquisition permitted by the Bush order went beyond FISA in a number of respects. For example, certain communications originating or received in the United States might be intercepted without warrant even though they were unambiguously covered by the FISA definition of "electronic surveillance."[70] The NSA could collect in the United States Internet content for foreign communications that simply "transited" U.S. electronic networks;[71] thus, communications between foreign nationals might be intercepted in the United States if they were using an email service that resides on U.S. territory, even if the interception also captured content involving U.S. "communicants" having a reasonable expectation of privacy.

After the warrantless surveillance of electronic communications content was divulged in The New York Times, President Bush acknowledged in a December 17, 2005 radio address what

---

[68] Id., at 8.

[69] Id.

[70] See text at notes ___, *supra*.

[71] FISA encompasses as "electronic surveillance": "the installation or use of an electronic, mechanical, or other surveillance device in the United States for monitoring to acquire information, other than from a wire or radio communication, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes." 18 U.S.C. 1801(f)(4). Internet traffic does not count as "wire . . . communication" because FISA defines "wire communication" as "any communication while it is being carried by a wire, cable, or other like connection furnished or operated by any person engaged as a common carrier in providing or operating such facilities for the transmission of interstate or foreign communications." 18 U.S.C. 1801(l). Because Internet service providers do not operate as "common carriers" in the provision of Internet service, the installation of an interception device in the United States for acquiring information from Internet providers that captures information that would be protected by the Fourth Amendment from warrantless seizure, is covered by this definition.

the Administration called the Terrorist Surveillance Program.[72] In addition, the Administration prepared two public full presentations of its legal position. The more extensive of these was a January 19, 2006 Justice Department memorandum of unattributed authorship, entitled, "Legal Authorities Supporting the Activities of the National Security Agency Described by the President."[73] In this memorandum, as in an earlier letter from Assistant Attorney General William Moscella to the leadership of the House and Senate Select Committees on Intelligence,[74] the Administration's legal stance rested to two essential propositions. The first is that warrantless electronic surveillance directed at al Qaeda and its supporters fell within the President's inherent war powers, as confirmed by the Authorization to Use Military Force in Afghanistan, or the AUMF,[75] enacted by Congress on September 12, 2001.[76] The second was that the President has inherent constitutional power to conduct the TSP no matter what the AUMF says and, if FISA is read to preclude this particular program of foreign intelligence surveillance, then FISA is unconstitutional.[77]

Although both propositions were highly problematic – the Office of Legal Counsel subsequently repudiated several aspects of its earlier legal memoranda that were the basis of this legal defense[78] – one could imagine at least a coherent argument on behalf of programs limited

---

[72] President George W. Bush, "President's Radio Address," 2005 WL 3450560 (Dec. 17, 2005), summarized in Jeffrey W. Seifert, Data Mining and Homeland Security: An Overview 23-24 (Congressional Research Service, Jan. 18, 2007), available at http://www.fas.org/sgp/crs/homesec/RL31798.pdf.

[73] U.S. Department of Justice, Legal Authorities Supporting the Activities of the National Security Agency Described by the President (Jan. 19, 2006), *reprinted in* David Cole and Martin S. Lederman, *The National Security Agency's Domestic Spying Program: Framing the Debate*, 81 Ind. L. Rev. 1355, 1374 (2006) (hereafter, "NSA Legal Authorities").

[74] Letter from William E. Moschella, Assistant Attorney General, Office of Legal Affairs, U.S. Department of Justice to the Leadership of the Senate Select Committee on Intelligence and the House Permanent Select Committee on Intelligence (Dec. 22, 2005), reprinted in Cole and Lederman, *supra* note 73, at 1360.

[75] Pub. L. No. 107-40, 15 Stat. 224 (2001) (hereafter, "AUMF").

[76] NSA Legal Authorities, *supra* note __, at 1379-90.

[77] Id., at 1407.

[78] Memorandum for the Files by Steven G. Bradbury, Principal Deputy Assistant Attorney General, Office of Legal Counsel re: Status of Certain OLC Opinions Issued in the Aftermath of the Terrorist Attacks of September 11, 2001 (Jan 15, 2009), available at http://www.justice.gov/opa/documents/memostatusolcopinions01152009.pdf;

to targeting communications to and from persons reasonably believed to be acting in Afghanistan or on behalf of al Qaeda. That defense, however, would be yet more dubious if extended to the NSA's metadata programs, which clearly and foreseeably reached millions of communications with no Afghanistan or al Qaeda connection. Although the New York Times stories, among others, did indicate in 2005 some sort of undisclosed NSA data mining program,[79] the Bush Administration's disclosures did not address its collection of metadata.[80]

The collection of telephony metadata gave the NSA information regarding the originating numbers and numbers called, as well as call duration, for apparently every telephone call made over the networks of cooperating telephone companies.[81] No requirement was imposed that limitations were imposed regarding the location of callers or participation of non-U.S. persons because the NSA did not acquire this information through government electronic surveillance.[82] This information is regularly collected by telephone companies for their own business purposes and was requested pursuant to the PATRIOT Act Section 215's authority for the acquisition of "tangible things," namely, business records.[83] As reported by the IG: "NSA determined that under the [2011 Presidential] Authorization it could gain access to approximately 81% of the international calls into and out of the United States through three corporate partners."[84]

---

see also PETER M. SHANE AND HAROLD H. BRUFF, SEPARATION OF POWERS LAW: CASES AND MATERIALS 718-719 (3d ed. 2011).

[79] Eric Lichtblau and James Risen, *supra* note 56.

[80] An electronic search of the Bush Administration's documents discussing the Terrorist Surveillance Program, cited in notes 73 and 74, *supra*, confirms that neither documents uses the words "metadata" or "Internet."

[81] Administration White Paper: Bulk Collection of Telephony Metadata Under Section 215 of the USA PATRIOT Act, at 3 (Aug. 9, 2013), available at http://big.assets.huffingtonpost.com/Section215.pdf.

[82] See, e.g., In Re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things From [Redacted], BR-1380, at 4 (FISC, Apr. 25, 2013) (ordering respondent to produce "all call detail records or 'telephony metadata' created by-for communications (i) between the United States and abroad; or (ii) wholly within the United States, including local telephone calls."), available at http://www.fas.org/irp/news/2013/07/215_order.pdf.

[83] Pub. L. 107–56, § 215, 115 Stat. 287 (2001), codified as amended at 50 U.S.C. § 1861(a).

[84] NSA IG Report, *supra* note 62, at 27.

Such metadata were then available to the NSA for what it called "contact chaining." As explained in the IG Report: "Contact chaining is the process of building a network graph that models the communication (e-mail, telephony, etc.) patterns of targeted entities (people, organizations, etc.) and their associates from the communications sent or received by the targets."[85] Furthermore:

> Additional chaining can be performed on the associates' contacts to determine patterns in the way a network of targets may communicate. Additional degrees of separation from the initial target are referred to as "hops." For example a direct contact is one hop away from the target. A contact of the direct contact would be described as being 2 hops away from the target. The resulting contact-graph is subsequently analyzed for intelligence and to develop potential investigative leads.[86]

Analysts would do contact chaining on the U.S. numbers to determine, for example, which numbers were linked to foreign numbers. As the IG recounts: "The records were used by NSA Counter-Terrorism metadata analysts to perform call chaining and network reconstruction between known al Qaeda and al Qaeda-affiliate telephone numbers and previously unknown telephone numbers with which they had been in contact."[87]

Until March, 2004, telephone companies were also providing the NSA metadata concerning Internet communications.[88] In March, 2004, however, the Justice Department's Office of Legal Counsel, under new leadership, determined that the collection of Internet metadata could not be squared with either FISA or the PATRIOT Act.[89] Although no memorandum of its advice has been made public, two propositions probably led to this conclusion.[90] First, because Internet metadata are not routinely kept by the cooperating

---

85 Id., at 13.
86 Id., at 13 n. 6.
87 Id., at 33.
88 Id., at 8, 32, 38.
89 Id., at 38.
90 Julian Sanchez, *What the Ashcroft "Hospital Showdown" on NSA spying was all about: How the government sought to justify blanket collection of Internet metadata*, ARSTECHNICA.COM (July 29 2013), available at http://arstechnica.com/tech-policy/2013/07/what-the-ashcroft-hospital-showdown-on-nsa-spying-was-all-about/.

companies, its acquisition would not fit under Section 215; collecting the metadata would amount to electronic surveillance. Second, because there was likely no way to exclude the collection of metadata from millions of emails from U.S. communicants, their bulk acquisition plainly violated the terms of FISA. In a much-publicized and dramatic episode, Attorney General Ashcroft, lying in a hospital bed, refused to sign off on President Bush's March 11, 2004 authorization for Internet metadata collection.[91] The NSA initially continued the interception anyway, based on approval by White House Counsel, rather than the Attorney General.[92] On March 26, 2004, however, President Bush temporarily discontinued the authorization for bulk Internet metadata collection.[93]

### 4. PATRIOT Act Amendments of 2006, the Protect America Act and the FISA Amendments of 1978

As noted above, President Bush's acknowledgement of NSA warrantless content collection programs did not precipitate anything like the extended public discussion and systematic congressional investigations that preceded the enactment of FISA – or that is occurring now in the wake of the Snowden leaks. Instead, the Administration proceeded to consult with the Foreign Intelligence Surveillance Court to develop rationales under which programs first developed under President Bush's 2001 order could be legitimated instead by orders of the FISC.

---

91 Daniel Klaidman, Stuart Taylor Jr. and Evan Thomas, "They were loyal conservatives, and Bush appointees. They fought a quiet battle to rein in the president's power in the war on terror. And they paid a price for it," NEWSWEEK, Feb. 6, 2006, at 34. Although the Newsweek article was the first to reveal the fact of a hospital pilgrimage, its full details later emerged through testimony by former Deputy Attorney General Comey to the Senate Judiciary Committee. Testimony of James B. Comey, Former Deputy Attorney General, U.S. Department of Justice to the Committee on the Judiciary, *Hearing on Preserving Prosecutorial Independence: Is the Department of Justice Politicizing the Hiring and Firing of U.S. Attorneys? – Part IV*, U.S. Senate, 110th Cong., 1st Sess. (2006), available at http://www.washingtonpost.com/wp-dyn/content/article/2007/05/15/AR2007051501043.html.

92 NSA IG Report, *supra* note 62, at 38.

93 Id., at 32.

The first of these transitions actually occurred with regard to the Internet metadata program that had been suspended in March, 2004. By July, 2004, the Administration was able to secure from the FISC a "pen register/trap and trace" order to permit the Internet metadata collection: "[T]he order essentially gave NSA the same authority to collect bulk Internet metadata that it had under the PSP, except that it specified the datalinks from which NSA could collect, and it limited the number of people that could access the data."[94]

As for telephony metadata, NSA acquisition was pursued under PATRIOT Act Section 215. On March 9, 2006, Congress enacted the "USA PATRIOT Improvement and Reauthorization Act of 2005," which amended Section 215 to require only that the "records [pursued under that section] are sought for an authorized investigation . . . to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities."[95] A FISC Order covering telephone metadata was instituted in May, 2006, producing no reduction in metadata acquisition, limiting only who could access the data and requiring somewhat more stringent oversight.[96]

---

[94] NSA IG Report, *supra* note 62, at 39. Although released in a form that redacted the date of issuance (!), the Undated Opinion by Judge Colleen Kollar-Kotelly Declassified Without Date or Caption (FISC), available at http://www.dni.gov/files/documents/1118/CLEANEDPRTT%201.pdf, reads as if it represents the original order. There are arguably three quite uncomfortable features of Judge Kollar-Kotelly's analysis. First, the pen register/trap and trace provisions of FISA, speak of applications to authorize "*a* pen register or trap and trace device," § 18 U.S.C. 1842(a)(1) (emphasis added), which might well suggest that Congress did not intend to authorize FISA to permit bulk acquisition of Internet (or any other) metadata under a single FISC order covering multiple devices. Second, although the court acknowledges that the vast majority of captured metadata will not be related to terrorism or foreign intelligence, id., at 48, Judge Kollar-Kotelly finds that the information sought is "relevant to an ongoing investigation to protect against international terrorism or clandestine intelligence activities," as FISA requires, § 18 U.S.C. 1842(c)(2), apparently because the metadata search is not too broad to satisfy the Fourth Amendment's reasonableness requirements – a seeming non sequitur. Id., at 50. Finally, the judge's order contains a series of requirements for the storage, accessing and dissemination of the acquired metadata, even though § 18 U.S.C. 1842 makes no provision for the judicial imposition of such conditions. Orin Kerr, *Problems with the FISC's Newly-Declassified Opinion on Bulk Collection of Internet Metadata*, LAWFARE (Nov. 19, 2013), available at http://www.lawfareblog.com/2013/11/problems-with-the-fiscs-newly-declassified-opinion-on-bulk-collection-of-internet-metadata/.

[95] Pub. L. 107–56, § 215, 115 Stat. 287 (2001), codified as amended at 50 U.S.C. §§1861.

[96] In re: Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things from [Redacted], BR06-05 (FISC, May 24, 2006), available at https://www.aclu.org/files/assets/pub_May%2024%202006%20Order%20from%20FISC.pdf.

The orders covering telephone and Internet content proved more complex because of the large volume of telephone numbers and email addresses – "selectors," in NSA parlance – that the NSA wanted to include. With regard to foreign "selectors," the NSA and Justice attempted to solve this problem in 2007 by changing "the traditional FISA definition of a 'facility' [to be targeted] as a specific telephone number or email address . . . to encompass the gateway or cable head that foreign targets use for communications."[97] Even this move, however, significantly reduced the number of target addresses available to the NSA. The documentation that the FISC demanded to justify the inclusion of specific selectors reduced the number of foreign addresses available from 11,000 to 3,000 and the number of domestic addresses to essentially just one.[98]

The unworkability of the FISC orders, especially for content, led the Administration in 2007 to seek amendments to FISA. Congress's initial, short-term solution was the Protect America Act of 2007.[99] The PAA:

> authorized the Director of National Intelligence and the Attorney General to acquire foreign intelligence information concerning persons outside the United States for one year, if the acquisition involved the assistance of a communication service provider, custodian or other person, and a significant purpose of the collection was the acquisition of foreign intelligence information. The Act was set to sunset after 180 days, on February 1, 2008.[100]

The PAA was highly controversial in a number of respects. For those skeptical of the TSP, the Act seemed to go too far in relaxing judicial oversight of electronic surveillance and creating

97 NSA IG Report, *supra* note 62, at 41.
98 Id., at 41-42.
99 Pub.L. 110-55, 121 Stat. 7 (2007).
100 S. Rept.100-209, 110th Cong., 1st Sess., at 6 (2007).

loopholes through which warrantless surveillance might be directed at persons within the United States.[101]

Congress ultimately replaced the PAA with the Foreign Intelligence Surveillance Act of 1978 Amendments of 2008.[102] The Amendments accomplished a number of key things. Among its more controversial sections, it provided a path to immunity from liability for telecommunications companies that may have violated FISA by cooperating with Bush Administration surveillance programs between 2001 and 2007.[103] Even more important for the future, however, Section 702 of the Amendments added a new title to FISA providing so-called, "Additional Procedures for Targeting Communications of Certain Persons Outside the United States,"[104] which were to remain in effect until December 31, 2012, but which have since been extended.[105] When a targeted individual is reasonably believed to be outside the United States, the Attorney General may apply for an order approving the acquisition from that person of foreign intelligence information under conditions slightly more relaxed than those specified by 50 U.S.C. §§ 1804 and 1805. For example, if the targeted person is "an officer or employee" of a foreign power, they need not themselves be a "foreign power," or an "agent of a former power."[106] Alternatively, when a targeted person is reasonably believed to be outside the United States, but the Attorney General wishes to conduct electronic surveillance of the target, or to acquire the target's stored electronic data or communications, within the United States, the Attorney General may seek an order from the FISC that not only approves the acquisition in

---

[101] See, e.g., *ACLU Fact Sheet on the "Police America Act,"* ACLU.ORG (Aug. 7, 2007), available at https://www.aclu.org/national-security/aclu-fact-sheet-%E2%80%9Cpolice-america-act.

[102] Pub. L. 110-261, 122 Stat. 2436 (2008).

[103] Id., at Title II, 122 Stat. 2467, codified at 50 U.S.C. §§ 1885a-1885c. For analysis, see Edward C. Liu, Retroactive Immunity Provided by the FISA Amendments Act of 2008 (Congressional Research Service, July 25, 2008), available at http://www.fas.org/sgp/crs/intel/RL34600.pdf.

[104] Id., Title I, at 122 Stat. 2437 (2008), codified at 50 U.S.C. §§ 1881-1881g.

[105] Foreign Intelligence Surveillance Act (FISA) Amendments Act Reauthorization Act of 2012, Pub. L. 112-238, 126 Stat. 1631 (2008).

[106] 50 U.S.C. § 1881c.

question, but compels the cooperation of private "electronic communication service providers" in the acquisition.[107]

The most dramatic new procedures, however, allow the Attorney General and the Director of National Intelligence to institute legally authorized programs of surveillance of up to one year "of persons reasonably believed to be located outside the United States."[108] Such programs do not require that targeted individuals be named to the FISC, but only that the Attorney General and the DNI certify that procedures are in place that are reasonably designed to limit surveillance to persons in general who are reasonably believed to be outside the United States, and that would prevent the intentional acquisition of communications among persons all of whom are known to be inside the United States.[109] It is required also that minimization procedures be in place[110] and that "a significant purpose" of the acquisition be obtaining foreign intelligence information.[111] The Attorney General and DNI may jointly initiate such acquisitions even without judicial certification if they jointly determine "that exigent circumstances exist because, without immediate implementation of an authorization. . ., intelligence important to the national security of the United States may be lost or not timely acquired and time does not permit the issuance" of a judicial order.[112] These procedures essentially eliminate the documentation complexities that made the FISC's 2007 orders on content acquisition impracticable from NSA's point of view. The new Section 702 also appears to eliminate the statutory barrier to the

107 50 U.S.C. § 1881b.
108 50 U.S.C. § 1881a.
109 50 U.S.C. § 1881a(g).
110 50 U.S.C. § 1881a(e)(1).
111 50 U.S.C. § 1881a(g)(2)(v).
112 50 U.S.C. § 1881a(c)(2).

collection of Internet metadata. Yet the Obama Administration reportedly shut down the program, for unspecified reasons, in 2011.[113]

### 5. The Snowden Revelations about Information Collection and Statutory Uncertainty: Segue to a Symposium

On June 5, 2013, The Guardian published the first of a stream of explosive news stories about NSA surveillance based on documents leaked by Edward Snowden, an employee of NSA contractor Booz Allen Hamilton.[114] The first document to be disclosed was a secret FISC order compelling a Verizon subsidiary to turn over call details for every domestic and international phone call placed on its network during a three-month period.[115] The Order made clear for the first time that the NSA was tracking metadata on the telephone communications of millions of Americans, not just suspected agents of a foreign power or terrorists.

A story published the next day revealed the existence of a computer system called PRISM, which – according to a set of leaked training slides – allows the Government to analyze information it collects from Microsoft, Google, Yahoo!, Faccbook, PalTalk, YouTube, Skype, AOL, and Apple.[116] This material includes "search history, the content of emails, file transfers and live chats."[117]

---

[113] Glenn Greenwald and Spencer Ackerman, "NSA collected US email records in bulk for more than two years under Obama," THE GUARDIAN (June 27, 2013), available at http://www.theguardian.com/world/2013/jun/27/nsa-data-mining-authorised-obama.

[114] Glenn Greenwald, *NSA collecting phone records of millions of Verizon customers daily*, THE GUARDIAN (June 5, 2013), available at http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order.

[115] In re: Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things from Verizon Business Network Services, Inc. on BEHALF of MCI Communication Services, Inc. D/B/A Verizon Business Services, BR-13-80 (FISC, Apr. 25, 2013), available at https://www.aclu.org/files/natsec/nsa/20130816/Section%20215%20-%20Secondary%20Order%20-%20Verizon.pdf.

[116] Glenn Greenwald and Ewen MacAskill, *NSA Prism program taps in to user data of Apple, Google and others*, The Guardian (June 6, 2013), available at http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data.

[117] PRISM/US-984XN Overview OR The SJGAD Used Most in NSA Reporting – Overview, Slide 3, available at https://www.aclu.org/files/natsec/nsa/20130816/PRISM%20Overview%20Powerpoint%20Slides.pdf.

The disclosure of these two programs involving the massive collection of both telephony metadata and online communications set the stage for what has been an extraordinary string of disclosures[118] – some in the press, some through government declassification – that have shed unprecedented light on the workings of our foreign intelligence surveillance regime. Among the document leaks are:

- NSA documents describing its "mission capabilities" based on the collection of metadata;
- FISC documents concerning NSA targeting and minimization procedures;
- Justice Department briefings to congressional committees concerning the nature of NSA collection programs;
- NSA documents concerning programs for collecting Internet and telephony data from fiber-optic cable networks;
- NSA documents on strategies to defeat encryption; and
- NSA documents revealing compliance problems in the implementation of collection programs subject to FISC orders.

For its part, the Government has produced or released declassified versions of an even larger number of documents. These include:

- correspondence with and testimony to Congress concerning the programs at issue, reflecting the system of congressional oversight;
- an Administration white paper on the bulk collection of telephony metadata under Section 215 of the PATRIOT Act;
- FISC opinions reviewing the NSA's bulk data collection programs; and

[118] My summaries of the kinds of documents either leaked or declassified is derived from the ACLU's online library of "NSA Documents Released to the Public Since June 2013," available at https://www.aclu.org/nsa-documents-released-public-june-2013. Summaries of key documents may also be found on LAWFARE, available at http://www.lawfareblog.com

- reports on the NSA's compliance with the FISC's Section 702 guidelines and minimization procedures;

Even in severely redacted form, the FISC opinions are especially intriguing. They display a court typically deferential to the Justice Department's statutory and constitutional arguments, but intensely engaged in the crafting and monitoring of the targeting and minimization requirements the court imposes under FISA. We learn that, at least on one instance, the court found aspects of the NSA's "upstream collection" of Internet transactions including multiple communications to be unlawful.[119]

Unsurprisingly given the magnitude of the programs now under scrutiny, the public's incomplete access to the assessments that drive these programs, and the extraordinary density of the documents to which we now have access, reactions to the Snowden revelations have differed markedly. Benjamin Wittes, a Brookings Institution senior fellow and editor-in-chief of the exceptional Lawfare blog, has written a generally sanguine assessment:

> [N]othing in the current disclosures should cause us to lose faith in the essential integrity of the post-Watergate system of delegated intelligence oversight. To the contrary, those disclosures should give the public great confidence both in the oversight mechanisms within the executive branch and in the judicial oversight mechanisms that review both the Section 215 collection program and the Section 702 collection program.
>
> The disclosures show no evidence of any intentional, unlawful spying on Americans or abuses of civil liberties. They show a low rate of the sort of errors any complex system of technical collection will inevitably yield. They show robust compliance procedures. They show earnest and serious efforts to keep the Congress informed—including members not on this committee or its counterpart in the House of Representatives. And they show an ongoing dialogue with the Foreign Intelligence Surveillance Court (FISC) about the parameters of the agency's legal authorities and a commitment both to keeping the court informed of activities and to complying with its judgments as to their legality. The FISC, meanwhile, in these documents looks nothing like the rubber stamp that it is portrayed to be in countless caricatures. It looks, rather, like a judicial institution of considerable energy, one whose oversight role with respect to

[119] [Redacted Caption], at 67-79 (FISC, Oct. 3, 2011), available at https://www.aclu.org/files/assets/fisc_opinion_10.3.2011.pdf.

> both Section 215 and Section 702 requires enormous time and energy on the part of the executive to satisfy.[120]

It is not hard to find less positive views. Jennifer Granick, director of civil liberties at the Stanford Center for Internet and Society and law professor Christopher Jon Sprigman, describe the NSA surveillance program as "criminal":

> The [NSA's bulk data] programs violate both the letter and the spirit of federal law. No statute explicitly authorizes mass surveillance. Through a series of legal contortions, the Obama administration has argued that Congress, since 9/11, intended to implicitly authorize mass surveillance. But this strategy mostly consists of wordplay, fear-mongering and a highly selective reading of the law.[121]

Law professor Marty Lederman, a former Obama Justice Department official, offers a mixed assessment of the FISC:

> The disclosures of the past several weeks have demonstrated, I think, that the FISC is extremely resolute, and careful, about ensuring that the NSA and FBI comply with the terms of the FISC's own orders, including the so-called "minimization" requirements–in part because the lawyers in . . . DOJ's National Security Division, take very seriously their responsibility to bring to the court's attention any compliance problems. When it comes to the more fundamental legal questions about the proper statutory and constitutional scope of a proposed program, however, the FISC process is not nearly as thorough or reliable, in large measure because the court hears from only one side.[122]

The aim of this symposium is to advance our national assessment of the NSA by looking at four key questions: the programs' legality, their contribution to national security, their impact on civil liberties, and possible avenues for constructive change. Professor John Yoo, whose defense of the Bush Administration surveillance programs proved controversial,[123] concludes

---

120 Prepared Statement of Benjamin Wittes Senior Fellow at the Brookings Institution before the Senate Select Committee on Intelligence, "Legislative Changes to the Foreign Intelligence Surveillance Act" (Sept. 26, 2013), at 2-3, available at http://www.lawfareblog.com/wp-content/uploads/2013/09/Wittes-SSCI-Hearing-Statement_Final-Draft_9.26.13.pdf.

121 Jennifer Stisa Granick and Christopher Jon Sprigman, *The Criminal N.S.A.*, N.Y. TIMES (June 27, 2013), available at http://www.nytimes.com/2013/06/28/opinion/the-criminal-nsa.html?_r=0.

122 Marty Lederman, *The Kris Paper, and the Problematic FISC Opinion on the Section 215 "Metadata" Collection Program*, JUST SECURITY (Oct. 1, 2013, updated Oct. 14, 2013), available at http://justsecurity.org/2013/10/01/kris-paper-legality-section-215-metadata-collection/.

123 The 2009 Unclassified PSP Report, *supra* note 60, criticizes Professor Yoo's legal opinions for giving insufficient weight to several provisions of FISA that would have appeared problematic for his conclusions, for

that the programs revealed by the Snowdon leaks are both constitutional and statutorily authorized.[124] Specifically, he finds that the metadata records acquired under Section 215 are "tangible things . . . relevant to an authorized investigation (other than a threat assessment) conducted in accordance with subsection (a)(2) to . . .protect against international terrorism," and thus clearly within purview of the statute.[125] The content collection programs under Section 702, because they target non-U.S. persons believed to be outside the U.S., likewise fall within the bounds of explicit statutory authority.[126]

Of the two statutory arguments, the Section 215 argument is clearly the more vulnerable – despite its acceptance by the FISC. As others have noted, "most of the information collected does not relate to individuals suspected of any wrongdoing."[127] The metadata can be viewed as relevant only under a needle-in-the-haystack theory – namely, that the likely existence of some modicum of specifically relevant data in the bulk collection makes all the records relevant because, at the moment of collection, it is impossible to be any more specific about what that modicum may be. This would seem to eliminate entirely the distinction between relevant and irrelevant records.[128]

---

failing to discuss Youngstown Sheet & Tube Co. v. Sawyer, 343 U.S. 579 (1952), as it might bear on his analysis, and for inaccuracies in his memos' descriptions of the activities being reviewed. Id., at 10-14. It perhaps ought be said, especially in the context of this symposium, that the constitutional analysis undergirding Professor Yoo's confidential professional advice is fully revealed in his academic writings both before and after his period of government service; he does not shy away from exposing his views to public critique.

[124] John Yoo, The Legality of the National Security Agency's Bulk Data Surveillance Programs, 9 ISJLP __ (2014).

[125] Id., at __.

[126] Id., at __.

[127] Laura K. Donohue, Bulk Metadata Collection: Statutory and Constitutional Considerations, at 50 (2013), available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2344774.

[128] For a detailed critical analysis of the Government's Section 215 argument, see id., at 48-64. For a comprehensive review of the interpretive issues raised under Section 215, see David S. Kris, *On the Bulk Collection of Tangible Things*, 1 LAWFARE RES. PAPER SERIES No. 4 (2013), available at http://www.lawfareblog.com/wp-content/uploads/2013/09/Lawfare-Research-Paper-Series-No.-4-2.pdf . The Administration's official defense of its position appears as Administration White Paper: Bulk Collection of Telephony Metadata Under Section 215 of the USA PATRIOT Act, at 3 (Aug. 9, 2013), available at http://big.assets.huffingtonpost.com/Section215.pdf.

Also, the use of Section 215 to elicit bulk metadata from telecommunications companies seems to run afoul of the strict statutory limits on the permissible disclosure to the government of telecommunication subscriber records.[129] 18 U.S.C. §2702(a) forbids "a provider of remote computing service or electronic communication service to the public [to] knowingly divulge a record or other information pertaining to a subscriber to or customer of such service . . . to any governmental entity." Section 2702(c) includes a number of exemptions to this prohibition, but none covers the blanket provision of business records.[130] The prohibition in §2702(a) was added by § 212(a)(1)(B) of the PATRIOT Act, the same statute that created the Section 215 "tangible things" authority.[131] The omission of a Section 215 exception to the Section 212 prohibition hardly seems like an oversight.[132]

---

[129] Donohue, *supra* note 127, at 63-64; Lederman, *supra* note 122.

[130] A provider described in subsection (a) may divulge the contents of a communication—

(1) to an addressee or intended recipient of such communication or an agent of such addressee or intended recipient;

(2) as otherwise authorized in section 2517, 2511 (2)(a), or 2703 of this title;

(3) with the lawful consent of the originator or an addressee or intended recipient of such communication, or the subscriber in the case of remote computing service;

(4) to a person employed or authorized or whose facilities are used to forward such communication to its destination;

(5) as may be necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service;

(6) to the National Center for Missing and Exploited Children, in connection with a report submitted thereto under section 2258A;

(7) to a law enforcement agency—

(A) if the contents—

(i) were inadvertently obtained by the service provider; and

(ii) appear to pertain to the commission of a crime; or

[(B) Repealed. Pub. L. 108–21, title V, § 508(b)(1)(A),Apr. 30, 2003, 117 Stat. 684]

(8) to a governmental entity, if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of communications relating to the emergency.

18 U.S.C. §2702(c).

[131] Pub. L. 107–56, 115 Stat. 272, 284 (2001).

[132] The FISC's handling of this issue seems flatly to ignore the plain statutory language. In re Production of Tangible Things From [REDACTED], Supplemental Opinion, BR 08-13, at 3 (FISC, Mar. 2, 2009), available at http://www.dni.gov/files/documents/section/pub_Dec%2012%202008%20Supplemental%20Opinions%20from%20the%20FISC.pdf. As summarized by Professor Lederman: "Judge Walton's analysis relied entirely on the fact that, under one of the exceptions to section 2702(c), the FBI can issue a 'national security letter' (NSL) to an electronic communications service provider, requesting that it disclose a customer's call records, without the approval or involvement of the FISC. See 18 U.S.C. 2709. Judge Walton reasoned that it would have been 'anomalous' for Congress to permit the Bureau to obtain such records from providers with a simple letter signed by an FBI official,

Much of the consternation bestirred by this statutory uncertainty has been devoted to the degree that the FISC's acquiescence in the Administration's arguments on behalf of Section 215 authority may reveal the weakness of a system of judicial oversight in which the surveillance target or his or her advocate never appear.[133] Targets become aware of their surveillance – and able to challenge it – only if subsequent criminal prosecution occurs and the government reveals the surveillance as a source of evidence against the defendant.[134] The possibility that the Government has systematically violated Congress's precise delimitation of its bulk acquisition authority has perhaps stirred less outrage than it otherwise might on the assumption that – with the Snowden revelations now before us – Congress will eventually determine yet more definitively whether bulk metadata collection of the kind so far undertaken should or should not be lawful.

The prospects for legislative reform, however, are presumably contingent also on the kinds of surveillance that the Constitution permits. Professor Yoo argues that the programs so far revealed pass Fourth Amendment muster either because the information acquired or the targets of investigation are beyond Fourth Amendment protection, and the searches embodied in these programs pass the test of reasonableness.[135] Like the Administration, Professor Yoo relies, in his Fourth Amendment defense of the metadata collection, on *Smith v. Maryland*,[136]

---

but to have prohibited the FBI from obtaining the same metadata with FISC approval and the oversight and minimization requirements prescribed by section 215." Lederman, *supra* note 122. The obvious problem with this analysis, as both Professors Lederman and Donohue note, Donohue, *supra* note 127, at 63-64, is that, however "anomalous" the statutory language may be, Judge Walton's analysis adds an additional exception to 18 U.S.C. §2702(c) that flies in the face of its terms and is nowhere supported by legislative history.

133 See Lederman, *supra* note 122.

134 The Justice Department is currently conducting a review of all criminal cases in which the government has used evidence gathered pursuant to FISA and may be notifying defendants in some of those cases that they were subjected to warrantless surveillance. Sari Horwitz, *Justice is reviewing criminal cases that used surveillance evidence gathered under FISA*, Wash. Post (Nov. 15, 2013), available at http://www.washingtonpost.com/world/national-security/justice-reviewing-criminal-cases-that-used-evidence-gathered-under-fisa-act/2013/11/15/0aea6420-4e0d-11e3-9890-a1e0997fb0c0_story.html.

135 Yoo, *supra* note 3, at ___.

136 442 US 735 (1979).

which held that the government did not need a warrant to track phone numbers because, in using telephone networks, callers voluntarily disclosed their numbers to a third party – namely, the phone company – thus eliminating the expectation of privacy. If *Smith* is fully applicable to the Section 215 orders, the Fourth Amendment does seem to have been decided in the Government's favor. Commentators who dissent rely chiefly on the concurring opinions of five Justices in the Supreme Court's recent decision forbidding the warrantless attachment of GPS tracking devices on private automobiles which indicated their openness to rethinking whether *Smith* ought to apply to searches for aggregate data.[137] So far, however, the Government's Fourth Amendment case seems plausibly grounded in precedent.

Professors Katherine Strandberg and Laura Donahue argue, however, that the programs Snowden revealed violate constitutional rights protections in other respects. In *Membership Lists, Metadata, and Freedom of Association's Specificity Requirement*,[138] Professor Strandberg argues that metadata surveillance is unconstitutional unless conducted in compliance with the First Amendment's guarantee of freedom of association. As analyzed by Professor Strandburg, that right entails certain specificity requirements that the current Section 215 programs do not meet. In *PRISM and the Interception of Communications Under Section 702 of the Foreign Intelligence Surveillance Act*,[139] Professor Laura Donohue argues, *Smith* notwithstanding, the NSA's Internet content surveillance program fails Fourth Amendment requirements. She agrees with Professor Yoo that the program is consistent with FISA, but argues that the program is unconstitutional because of the compulsory involvement of private telecom companies and the

[137] United States v. Jones, 565 US ___, 132 S.Ct. 945, 954 (2012) (Sotomayor, J., concurring); id., at 957 (Alito, J., concurring).
[138] 9 ISJLP ___ (2014).
[139] 9 ISJLP ___ (2014).

failure to prevent overbreadth. She concludes that the interception of all international communications fails the reasonableness test of *Katz*.

For many Americans, the wisdom or imprudence of the NSA programs will depend less on legal argument and more on what NSA surveillance contributes to or detracts from national security and civil liberties. Mark D. Young, who serves as a Senior Advisor in the United States Cyber Command Directorate for Plans and Policy – and who was formerly Special Counsel for Defense Intelligence for the House Permanent Select Committee on Intelligence – argues both that the programs are important and that the Snowden leaks have compromised U.S. national security in four areas: facilitating operational adjustments in the techniques and security practices of our adversaries; complicating U.S. foreign relations; impairing important cooperation between the U.S. government and private industry; and unjustifiably reducing public confidence in the National Security Agency, with likely negative impacts on its resources and authorities.[140]

For their part, however, political scientists John Mueller and Mark G. Stewart seriously question both the need for secrecy and whether the metadata program, in particular, is truly justified on a national security basis.[141] Their review of the program's claimed successes lead them to conclude that the program "would very likely fail a full cost-benefit analysis handily even without taking into consideration privacy and civil liberties concerns."[142] The debate framed by these two pieces could hardly be more important.

The debate over civil liberties might well seem one-sided – surveillance would not seem to offer any immediate civil liberties advantages – although proponents of NSA surveillance may assert that surveillance serves the cause of civil liberties in an indirect, but important way. It

---

[140] Mark D. Young, *National Insecurity: The Impacts of Illegal Disclosures of Classified Information*, 9 ISJLP ___ (2014).

[141] John Mueller and Mark G. Stewart, *Secret without Reason and Costly without Accomplishment: Questioning the NSA's Metadata Program*, 9 ISJLP ___ (2014).

[142] Id., at ___.

could be argued, if the programs help the government to fend off terrorist attack, they necessarily help to promote an atmosphere of public calm that is more conducive to respect for civil liberties. Speaking of even the limited oversight provided by the FISC, David Addington, Vice President Cheney's Chief of Staff, predicted: "We're just one bomb away from getting rid of that obnoxious court."[143] Even though Mr. Addington's words may have created what one hopes is the inadvertent impression that he would have welcomed that attack, our history after 9/11 reinforces the fundamental point that the public is more vigilant about its civil liberties when it feels safe.

For civil libertarians, however, any such argument is quite likely to pale given the more direct civil liberties impacts of mass surveillance. In *NSA Surveillance: The Implications for Civil Liberties*, Shayana Kadidal, the senior managing attorney of the Guantánamo Global Justice Initiative at the Center for Constitutional Rights in New York City, asserts that such programs threaten the very independence of citizen thought and action that are central to democratic governance.[144] He illustrates that idea concretely by explaining the impact of the NSA programs on his own work and on the work of other lawyers who represent politically unpopular or vulnerable clients. Like Professors Mueller and Stewart, he also calls into question the "liberty-security tradeoff" meme. Like them, he calls into question the few successes publicly identified with the NSA programs and worries, as they do, that the extraordinary rate of false positives means that the FBI is too often spending significant time and effort on leads that go nowhere.[145]

---

143 JACK GOLDSMITH, THE TERROR PRESIDENCY: LAW AND JUDGMENT INSIDE THE BUSH ADMINISTRATION 181 (2007).

144 9 ISJLP ___ (2014).

145 Id., at ___.

Bryce Newell, who is both an attorney and a doctoral student in information science, places the civil liberties question in a more theoretical frame.[146] Taking what he calls a "neo-republican" stance on the nature of liberty – namely, that liberty manifests itself in the ability of a people to self-govern, by reducing domination and the arbitrary exercise of power – Newell argues that surveillance is not necessarily inimical to liberty per se. Its legitimacy, however, requires that it be exercised for the public good and that the public have meaningful opportunities to challenge the secrecy in government that may prevent people from exercising genuine democratic oversight and control over their political representatives. He finds that idea honored more robustly in relevant decisions of the European Court of Human Rights than in U.S. courts, whose resistance to secrecy challenges he criticizes.

Given serious concerns from multiple angles that the Snowden leaks and accompanying document declassification have evoked, the issue is finally imposed: how might matters be improved?

Professor Nathan Sales, whose government service most recently includes a stint as Deputy Assistant Secretary for Policy Development in the Bush Department of Homeland Security, advocates the establishment of what he calls baseline rules for conducting "programmatic surveillance."[147] More than a number of other authors in this volume, he credits the value of such surveillance and thinks it unlikely to disappear. It is therefore perhaps unsurprising that he believes the NSA, as currently operating, already respects – though perhaps imperfectly – the baseline principles he identifies. He does advocate that metadata surveillance be continued on the basis of clearer and more explicit statutory authority in order to maximize

[146] Bryce Clayton Newell, *The Massive Metadata Machine: Liberty, Power, and Secret Mass Surveillance in the U.S. and Europe*, 9 ISJLP ___ (2014).

[147] Nathan Alexander Sales, *Domesticating Programmatic Surveillance: Some Thoughts on the NSA Controversy*, 9 ISJLP ___ (2014).

the potential for both effective congressional and judicial oversight. He would also like to see debates over the adoption of such programs become more transparent to the public and better informed. Perhaps his most innovative suggestion is building into the surveillance system technological safeguards that "*technological safeguards* that protect privacy and civil liberties by restricting access to sensitive information and tracking what officials do with it."[148]

For his part, Professor Stephen Vladeck – although perhaps less sanguine about programmatic surveillance than Professor Sales – takes a cautionary stance on the potential for intensifying judicial review.[149] Post-9/11 litigation has been severely hamstrung by a combination of standing problems and the state secrets doctrine. Even if Congress enacted a workaround for the standing, it is not clear how routinely plaintiffs could challenge NSA programs absent a steady stream of further leaks. Proposals to make FISC hearings more adversarial hold more promise, but it remains unclear whether Article III would permit a designated advocate to appeal FISC orders to a higher court or whether it is possible to conduct an effectively adversarial system consistent with the level of secrecy that a system of foreign intelligence surveillance might well require.

Former FCC Chairman Reed Hundt takes a rather different tack.[150] No doubt reflecting his knowledge as a former telecommunications regulator, Mr. Hundt is careful to cast what most are calling NSA surveillance as a collaborative project between government and the private sector. He is emphatically concerned about the prospects for a kind of "corporatism" he thinks inimical to "both economic and social freedom."[151] Mr. Hundt argues that it is, in fact, secrecy, rather than the fact of surveillance that is the fundamental problem with the current system. He

148 Id., at ___.
149 Stephen I. Vladeck, *Standing and Secret Surveillance,* 9 ISJLP ___ (2014).
150 Reed E. Hundt, *Making No Secrets About It*, 9 ISJLP ___ (2014).
151 Id., at ___.

proposes an ambitious list of reforms aimed at increasing what individuals know about their own targeting and what the public knows about the scope of government programs, past and present. Although his menu of suggestions includes an expansion of warrant requirements, the weight of his argument really goes to the public-ness of what the government is doing, reducing the likelihood of abuse once information has been collected, and better managing what could be the mind-boggling expense of managing security in the digital domain – what Mr. Hundt calls "the staggering expenditures of government funds."[152]

Hovering quite conspicuously over all these important questions is whether what might be called the "cybernation" of information – that is, the revolution in the digitizing of information with its profound impacts on information storage, processing, and dissemination – requires a comprehensive rethinking of the value, nature, and protection of privacy. It is thus fitting that our concluding essay, by the eminent sociologist Amitai Etzioni, elaborates what its author takes to four core principles of what he calls a liberal communitarian approach to cyber age privacy, along with a host of possible operational implications.[153] His paper functions as an invitation to view the NSA disclosures as an occasion for embracing a yet wider view, taking a systematic look at the principles we would wish to guide information policy in the cyber age.

### 6. A Concluding Note about Executive Power

The Snowden leaks and the subsequent Obama Administration declassifications have pointedly refocused Congress's attention on the prospects for FISA reform. Both our elected branches appear to be acting on the assumption that whatever legislation emerges will actually

---

[152] Id., at ___.

[153] Amitai Etzioni, *A Cyber Age Privacy Doctrine: A Liberal Communitarian Approach*, 9 ISJLP ___ (2014).

govern how the NSA operates[154] – whether its operations are affirmed in their current scope, legislatively restricted, or, least likely, authorized in yet more expansive terms. Professor Yoo, however, advances in his paper a theory of executive authority that also underlay his legal advice as a government official – a theory that casts significant doubt on the imperative of legislative observance by the executive branch. The core premise of his argument is as follows:

> The Constitution vests the President with the executive power and designates him Commander-in-Chief. The Framers understood these powers to place the duty on the executive to protect the nation from foreign attack and the right to control the conduct of military hostilities. To exercise that power effectively, the President must have the ability to engage in electronic surveillance that gathers intelligence on the enemy.[155]

Professor Yoo argues that it follows from this position that the President does not need legislative authorization to conduct such surveillance as he deems necessary to protect the United States against foreign enemies; it follows further, in his view, that Congress may not place any binding limitations on that authority. The function of FISA, as Professor Yoo construes the Constitution, is neither to enable, nor to limit national security surveillance per se; it is only to prescribe a legal safe harbor within which the executive branch may both engage in national security surveillance and use its fruits as evidence in any criminal prosecutions that ensue.[156]

A great deal is packed into that argument, which is important to disentangle. First, putting aside controversial issues surrounding the supposition of presidential authority to determine with whom we are "at war" and of the consequent scope of commander-in-chief authority, it strikes me as quite plausible that the founding generation understood "executive power" to include some tacit authority to engage in intelligence work against foreign powers. After all, neither the durability of the new nation, nor even the congenial reception of other

---

[154] The Obama Administration is notably more reluctant than its predecessor to assert presidential power, even in national security setting, to act beyond what Congress enacts by way of statutory authority. Peter M. Shane, Executive Power, the Rule of Law and the Obama Administration (unpublished manuscript).

[155] Yoo, *supra* note 3, at ___ (footnotes omitted).

[156] Id., at ___.

nations to the United States could be taken for granted in 1789. It is reasonable that the framers themselves would have read Article II as empowering the President to keep tabs on foreign powers and their agents as part of his inherent national security portfolio.

It does not follow from that observation, however, that the President would be deemed to have exclusive power beyond the regulatory authority of Congress to engage in the surveillance of Americans, especially in the absence of declared war. Even if some such power might be thought to exist absent a legislative charter, Congress's undoubted authority to regulate our networks of electronic communication give it the right, at its discretion, to legislate the circumstances under which Americans may be brought within the government's surveillance umbrella. There is no doubt that this is what Congress thought it was doing when it enacted the original FISA.[157]

Prior to FISA, when Congress enacted its Title III procedure for criminal surveillance warrants after the *Katz* decision, Congress provided that "nothing contained in [Title III] or in section 605 of the Communications Act of 1934 shall limit the constitutional power of the President . . . to obtain foreign intelligence information deemed essential to the security of the United States."[158] But FISA replaced that statement with language dictating that FISA and the criminal code would be henceforth the "exclusive means" of conducting electronic surveillance. Congress amended the criminal code to read in unambiguous terms: "[P]rocedures in this chapter or chapter 121 and the Foreign Intelligence Surveillance Act of 1978 shall be the

---

157 "The conferees agree that the establishment by this act of exclusive means by which the President may conduct electronic surveillance does not foreclose a different decision by the Supreme Court. The intent of the conferees is to apply the standard set forth in Justice Jackson's concurring opinion in the Steel Seizure Case: 'When a president takes measures incompatible with the express or implied will of congress, his power is at the lowest ebb, for then he can rely only upon his own constitutional power minus any constitutional power of congress over the matter.' *Youngstown Sheet and Tube Co. v. Sawyer*, 343 U.S. 579, 637 (1952)." Foreign Intelligence Surveillance Act of 1978 Conference Report, H.Rept. No. 95-1720, 95th Cong., 2d Sess. at 35.

158 Pub. L. 90–351, title III, § 802, 82 Stat. 213 (1968), repealed, Pub. L. 95–511, title II, § 201(a)–(c), 92 Stat. 1797 (1978).

exclusive means by which electronic surveillance, as defined in section 101 of such Act, and the interception of domestic wire, oral, and electronic communications may be conducted."[159] Congress had been confirmed in its authority to impose such a limitation by two Attorneys General, Edward Levi and Griffin Bell.[160]

Congress repeated its position in enacting the FISA Amendments Act of 2008. In the face of Justice Department opinions appearing to suggest either that FISA had not definitively limited the executive branch's surveillance authority or that the post-9/11 AUMF had implicitly augmented that authority, Congress reasserted the exclusivity point in Title 50 of the United States Code as well. FISA now reiterates the strict limitations on those statutory sources of authority on which the executive may rely to support electronic surveillance and adds that any additional authorities may be found only through subsequent "express statutory authorization," not through mere implication.[161]

It is imperative as a matter of democratic, constitutional self-governance that the executive branch acquiesce in Congress's view. Indeed, it may be this point – as much as the ex parte nature of FISC proceedings – that explains the seemingly odd disjuncture, noted above, between the FISC's apparent super-indulgence of counterintuitive statutory interpretations by the executive branch and its vigilance in the design and monitoring of provisions for minimization and other matters of implementation. That is, by accepting executive branch statutory interpretations that bring its surveillance activities within the purview of statute, the court accomplishes two things it might well consider important from a "rule of law" point of view. First, it avoids sensitive questions of whether, notwithstanding FISA, the executive could pursue certain kinds of surveillance under inherent Article II authority – authority that the FISC would

159 Pub. L. 95–511, title II, § 201(a)–(c), 92 Stat. 1797 (1978), codified at 18 U.S.C. § 2511(2)(f).
160 H.R. Rep. No. 95-1283, pt. 1, at 24 (1978).
161 Pub. L. 110–261, title I, § 102(a), 122 Stat. 2459, codified at 50 U.S.C. § 1812.

not be entitled to supervise. Second, the statutory rubric authorizes the FISC to impose limiting implementation requirements in the name of privacy which the court does monitor rigorously and in which the executive acquiesces – even, as with regard to bulk telephone records, where the court's authority to impose such requirements might be deemed questionable.

The FISC's institutional compromise, if I have correctly identified it, is hardly perfect. Its acquiescence in novel statutory interpretations looks like a disservice to a Congress that remains largely ignorant of those interpretations. The public forum surrounding legislative authorization is likely to be the only meaningful occasion for public deliberation on the proper contours for programs of electronic surveillance because there is quite likely to be no other context in which the executive branch will publicize the scope of what it thinks it needs to protect national security. If the FISC creates secret and unanticipated readings of Congress's handiwork, the value of such public deliberation is plainly called into question. But, as I have argued elsewhere, an executive branch that thinks its authority limited only by its unilateral assessments of its inherent discretionary powers is far more likely to overreach than an executive that thinks itself beholden to legislative authorization.[162] By helping to stabilize government surveillance practice within a statutory framework, the FISC is doing significant work.

In the 1970s, it was the Church Committee that lent impetus to both the reorganization of intelligence oversight in Congress and eventual enactment of FISA. Its investigation created a historical record that Americans could rely on as a basis for democratic debate about national security and intelligence gathering. Something similar should have happened in 2005-2006, when revelations about the Bush Administration made clear that government lawyers thought FISA did not constrain them. Instead, for better or worse – perhaps both – the official inquiry

[162] PETER M. SHANE, MADISON'S NIGHTMARE: EXECUTIVE POWER AND THE THREAT TO AMERICAN DEMOCRACY 113-142 and passim (2009).

and public debate that should have preceded amendments to FISA instead were triggered only by massive unauthorized leaks that revealed NSA surveillance of staggering scope. The implications of the current debate are plainly profound for both our future security and long-cherished American values. It remains to be seen whether our national institutions are up to the challenge.

Preliminary Draft 2.0 – Please Do Not Cite Without Permission
To be Published in *I/S: A Journal of Law and Policy for the Information Society*
9 ISJLP ___ (2014).
http://www.is-journal.org

# The Legality of the National Security Agency's Bulk Data Surveillance Programs

John Yoo*

Controversy has arisen again over the federal government's electronic surveillance efforts to gather intelligence on foreign terrorist groups. Recent disclosures, both authorized and illicit, have described two secret National Security Agency (NSA) programs. The first collects telephone "metadata" such as calling records—but not the content of phone calls—both inside and outside the United States. A second NSA program intercepts the e-mails of non U.S. persons outside the United States.[1] Despite the claims of critics, these programs do not violate the Foreign Intelligence Surveillance Act (FISA), as recently amended by Congress, or the Fourth Amendment to the Constitution. Concerns about the proper balance between these surveillance programs and individual privacy may be appropriate, but they properly fall within the province of Congress and the President to set future national security policy.

Legal questions over surveillance arise from the unconventional nature of the war against al Qaeda. On September 11, 2001, the al Qaeda terrorist network launched attacks on New York City and Washington, D.C. from territory in Afghanistan substantially under its control. Under normal circumstances, American military and intelligence officers, acting pursuant to the President's Commander-in-Chief authority, would carry out electronic surveillance against a foreign enemy in wartime. Al Qaeda, however, operates through teams of covert agents who disguise their communications and movements within normal peaceful activities. American law subjects domestic criminal enterprises, which operate in similar ways, to the more elaborate system of search warrants, individualized suspicion, and judicial supervision required by the Fourth Amendment. Controversy over the legality of the NSA's programs basically centers on

* Emanuel S. Heller Professor of Law, University of California, Berkeley Law School; Visiting Scholar, American Enterprise Institute. I thank Jesse Choper and Peter Shane for their comments. Lianna Bash and Steven Erkel provided outstanding research assistance.

[1] See, e.g., National Security Agency, The National Security Agency: Missions, Authorities, Oversight and Partnerships (Aug. 9, 2013); Barak Obama, President of the United States of America, President Obama Holds a Press Conference (Aug. 9, 2013), http://www.whitehouse.gov/photos-and-video/video/2013/08/09/president-obama-holds-press-conference. An up-to-date catalogue of the declassified documents can be found at: http://www.odni.gov/index.php/newsroom/press-releases/191-press-releases-2013/915-dni-declassifies-intelligence-community-documents-regarding-collection-under-section-702-of-the-foreign-intelligence-surveillance-act-fisa.

whether surveillance of al Qaeda should follow the wartime/foreign intelligence model or the criminal justice approach.

This paper will address the legality of the NSA's programs in this light. Part I will describe the surveillance efforts against al Qaeda within a broader historical and legal context. Part II will argue that the programs, as described publicly by authoritative sources, appear to meet statutory requirements. Part III will address whether the NSA programs are constitutional along two dimensions. It will argue that even if some aspect of the NSA programs does not fall within Congress's authorization for foreign intelligence and counter-terrorism surveillance, it would most likely rest within the President's Commander-in-Chief authority over the management of war. Second, even if the federal government has the internal authority to conduct surveillance, the Bill of Rights, through the Fourth Amendment, may still prohibit its application to citizens or non-citizens present in the territorial United States. Part III will argue, however, that the NSA programs do not violate the Fourth Amendment, as currently interpreted by the federal courts.

## I.

On September 11, 2001, the al Qaeda network launched four coordinated attacks aimed at critical buildings in the heart of the nation's capital and financial system. Nineteen terrorists hijacked four civilian passenger airliners and crashed them into the World Trade Center towers in New York City and the Pentagon outside Washington, D.C. Another flight, apparently destined for Congress or the White House, fell in Pennsylvania after passengers fought to seize back control of the plane. The attacks killed about 3,000 people, with many more injured, caused billions of dollars in physical damage, and caused further economic loss due to disruptions in transportation, communications, and the financial markets. If a nation-state, such as the Soviet Union during the Cold War, had carried out the identical strikes, there would be little doubt that the United States would be at war.

These attacks, however, significantly differed from a normal attack in a conventional war. The enemy's soldiers did not wear uniforms, did not carry arms openly, and did not operate as part of regular military units. Mohammed Atta and his eighteen agents disguised themselves as civilians for travel and training, used civilian aircraft as weapons, and launched the attacks by surprise from within U.S. borders. Al Qaeda itself cannot lay claim to the status of a nation. In 2001, it exercised no territorial sovereignty, it had no population, and fielded no regular armed forces. Rather, al Qaeda takes the form of a decentralized network of extremists who wish to engineer fundamentalist political and social change in Islamic countries. Its terrorist cells operate both abroad and within the United States.

It is al Qaeda's nature as a decentralized network that pressures the normal division between military and intelligence surveillance and the warrant-based approach of the criminal justice system. The Constitution vests the President with the executive power

and designates him Commander-in-Chief.[2] The Framers understood these powers to place the duty on the executive to protect the nation from foreign attack and the right to control the conduct of military hostilities.[3] To exercise that power effectively, the President must have the ability to engage in electronic surveillance that gathers intelligence on the enemy. Regular military intelligence need not follow standards of probable cause for a warrant or reasonableness for a search, just as the use of force against the enemy does not have to comply with the Fourth Amendment. During war, military signals intelligence might throw out a broad net to capture all communications within a certain area or by an enemy nation. Unlike the criminal justice system, which seeks to detain criminals, protection of national security need not rest on particularized suspicion of a specific individual.

This approach applies to national security activity that occurs within the United States as well as outside it. In 1972, the Supreme Court refused to subject surveillance for national security purposes to the Fourth Amendment warrant requirement.[4] It has extended these protections to purely domestic terrorist groups, out of concern that the government might use its powers to suppress political liberties. Lower courts, however, have found that when the government conducts a search of a foreign power or its agents, it need not meet the requirements that apply to criminal law enforcement. In a leading 1980 case, the Fourth Circuit held that "the needs of the executive are so compelling in the area of foreign intelligence, unlike the area of domestic security, that a uniform warrant requirement would unduly frustrate the President in carrying out his foreign affairs responsibilities."[5] A warrant for national security searches would reduce the flexibility of the executive branch, which possesses "unparalleled expertise to make the decision whether to conduct foreign intelligence surveillance" and is "constitutionally designated as the pre-eminent authority in foreign affairs."[6] A warrant requirement would place the national security decisions in the hands of the judiciary, which "is largely inexperienced in making the delicate and complex decisions that lie behind foreign intelligence surveillance."[7]

Under this framework, Presidents had conducted national security surveillance under their executive authority for decades. President Nixon's abuses, however, led

---

[2] U.S. Const. art. II.

[3] See, The Federalist No. 70, at 471-72 (Alexander Hamilton) (Jacob Cooke ed., 1961) ("Energy in the executive. . . is essential to the protection of the community against foreign attacks."); The Federalist No. 74, at 500 (Alexander Hamilton) (Jacob E. Cooke ed., 1961) ("Of all the cares or concerns of government, the direction of war most peculiarly demands those qualities which distinguish the exercise of power by a single hand."). See also John Yoo, The Powers of War and Peace: The Constitution and Foreign Affairs After 9/11, at 143-81 (2005)

[4] United States v. United States District Court, 407 U.S. 297, 322 (1972).

[5] United States v. Truong Dinh Hung, 629 F.2d 908, 913 (4th Cir. 1980).

[6] Id. at 913-14.

[7] Id.

Congress to enact the Foreign Intelligence Surveillance Act (FISA) in 1978.[8] FISA replaced presidentially-ordered monitoring of national security threats with a system similar to that used by law enforcement to conduct electronic surveillance of criminal suspects, but with important differences to protect classified information. FISA requires the government to show "probable cause" that a target is "an agent of a foreign power," which includes terrorist groups.[9] A special court of federal district judges, the Foreign Intelligence Surveillance Court (FISC) examines classified information in a closed, ex parte hearing, before issuing the warrant.[10]

FISA obviously strikes a compromise between the wartime and criminal approaches to information gathering. It establishes a system that bears strong resemblances to the criminal justice system, such as the requirement of an individual target, probable cause, and a warrant issued by a federal court. On the other hand, in a nod to the purposes of foreign intelligence surveillance, it does not require a showing of probable cause of criminal activity by the target, which the Fourth Amendment normally requires for a search warrant.[11] Instead, FISA only demands that the government show "probable cause" that the target is linked to a foreign power or terrorist group.

The Patriot Act of 2001 made important changes to FISA which bear directly on the legality of the NSA surveillance programs. Section 215 of the Patriot Act allows the government to seek an order from the FISC to a private party for "tangible things," which includes "books, records, papers, documents, and other items."[12] The government can obtain the records for two purposes: either for "an investigation to obtain foreign intelligence information not concerning a United States person" or "to protect against international terrorism or clandestine intelligence activities," so long as it does not infringe on First Amendment-protected activity.[13] To obtain the order, the government must show that "there are reasonable grounds to believe" that the records are "relevant" to "an authorized investigation."[14] An investigation is presumptively authorized if the records are related to "the activities of a suspected agent of a foreign power" or someone in contact with such an agent.[15]

Section 215 does not contain a revolutionary grant of authority to the government. It is akin to a grand jury subpoena for financial, communication, or travel records as part of a criminal investigation. In fact, the statute additionally defines the records as those that can be obtained by a subpoena issued by a federal court as part of a grand jury

---

[8] Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95-511, 92 Stat. 1783 (codified at 50 U.S.C. § 1801 et seq.).
[9] 50 U.S.C. § 1805(a)(2).
[10] 50 U.S.C. § 1805.
[11] See, e.g., Illinois v. Gates, 462 U.S. 213 (1983).
[12] USA Patriot Act, Pub. L. No. 107-56, 115 Stat. 272 (codified at 50 U.S.C. §1861 (2001)).
[13] §1861(a)(1).
[14] §1861(b)(2)(A).
[15] §1861(b)(2)(A)(ii).

investigation.[16] Section 215 of the Patriot Act provides the authority for the NSA's collection of telephone billing records. The NSA collects the data containing the phone numbers on both ends of a call, and the duration of every call made in the United States.[17] But it does not intercept the content of the call nor does it know the identity of the subscriber.[18] It collects the information into a database of all calls in the nation, which did not exist beforehand due to multiple telecommunications companies and their deletion of the records.[19] NSA purges records that are more than five years old.[20] A database allows NSA to quickly determine the calling chain of any overseas numbers discovered to belong to al Qaeda operatives. Once NSA tracks down the phone numbers called within the United States from a suspected al Qaeda phone number, it can then seek a warrant from the FISC to place the number under further surveillance and to collect other records, such as financial and travel information.

II.

As business records, phone call metadata falls within Section 215's definition of tangible items. It relates to an authorized investigation to protect against international terrorism. Several investigations into al Qaeda plots remain open, as shown by the repeated indictments against bomb plotters in the last five years, and the examination of records also helps protect the nation against terrorist attack. According to the NSA, only the information contained in the billing records is collected; the content of calls are not.[21] There can be no First Amendment violation if the content of the calls remains untouched. A critic might argue that the terms of the search are too broad, because 99 percent of the calls are unconnected to terrorism. An intelligence search, as Judge Richard Posner has described it, "is a search for a needle in a haystack."[22] Rather than focus on foreign agents who are already known, counter-terrorism agencies must search for clues among millions of potentially innocent connections, communications, and links. "The intelligence services," Posner writes, "must cast a wide net with a fine mesh to catch the clues that may enable the next attack to be prevented."[23] For this reason, the FISC approved the NSA program in 2006 and has continued to renew it since.[24]

---

[16] § 1861(c)(2)(D).
[17] Steven G. Bradbury, Understanding the NSA Programs: Bulk Acquisition of Telephone Metadata Under Section 215 and Foreign-Targed Collection Under Section 702, 1 Lawfare Res. Pap. Ser. 1, 2 (2013).
[18] Id.
[19] Id.
[20] Id. at 3.
[21] Report on the National Security Agency's Bulk Collection Programs Affected by USA PATRIOT Act Reauthorization, Dec. 14, 2009, at 3, available at https://www.fas.org/irp/news/2013/07/2009_bulk.pdf.
[22] Richard Posner, A New Surveillance Act, Wall St. J., Feb. 15, 2006, at A16; see also Richard Posner, Preventing Surprise Attacks (2005).
[23] A New Surveillance Act, supra note 13.
[24] Bradbury, supra note 17, at 2.

Members of the al Qaeda network can be detected, with good intelligence work or luck, by examining phone and e-mail communications, as well as evidence of joint travel, shared assets, common histories or families, meetings, and so on.[25] As the time for an attack nears, "chatter" on this network will increase as operatives communicate to coordinate plans, move and position assets, and conduct reconnaissance of targets.[26] When our intelligence agents successfully locate or capture an al Qaeda member, they must be able to move quickly to follow new information to other operatives before news of the capture causes them to disappear. The database created by the NSA is particularly important because it will point the way to al Qaeda agents within the United States, where they are closest to their targets and able to inflict the most harm on civilians.

The 9/11 hijackers themselves provide an example of the way that the NSA could correlate business record information to locate an al Qaeda cell. Links suggested by commercially available data might have turned up ties between each of the al Qaeda plotters and Khalid al Mihdhar and Nawar al Hazmi, the two hijackers known to the CIA in the summer of 2001 to have been in the country.[27] Mihdhar and Hazmi had rented apartments in their own name and were listed in the San Diego phone book.[28] Both Mohammad Atta, the leader of the 9/11 al Qaeda cell, and Marwan al-Shehi, who piloted one of planes into the World Trade Center, had lived there with them.[29] Hijacker Majed Moqed used the same frequent flier number as Hazmi; five hijackers used the same phone number as Atta when booking their flights; the remaining hijackers shared addresses or phone numbers with one of those hijackers, Ahmed Alghamdi, who was in the United States in violation of his visa at the time.[30]

Our intelligence agents, in fact, had strong leads that could conceivably have led them to all the hijackers before 9/11.[31] CIA agents had identified Mihdhar as a likely al Qaeda operative because he was spotted at a meeting in Kuala Lumpur and mentioned in Middle East intercepts as part of an al Qaeda "cadre."[32] Hazmi too was known as likely to be al Qaeda.[33] But in neither case was there enough evidence for a criminal arrest, because they had not violated any American laws. If our intelligence services had been able to immediately track their cell phone calls and email, it is possible that enough of the hijacking team could have been rounded up to avert 9/11.[34] Our task is much more

---

[25] See NAT 'L COMM 'N ON TERRORIST ATTACKS UPON THE U.S., THE 9/11 COMMISSION REPORT 47, 361-98 (2004), id. at 227 n.68 (noting that the United Arab Emirates was able to track Marwan al Shehhi, one of the future 9/11 hijackers when he contacted his family).
[26] See id. at 263-65.
[27] Heather MacDonald, What We Don't Know Can Hurt Us, City Journal, Spring 2004.
[28] Id.
[29] Id.
[30] Id.
[31] Id.
[32] 9/11 COMMISSION REPORT, supra note 15, at 158, 181.
[33] See id. at 158-59, 181-82.
[34] Id. at 272.

difficult today, because we might not have even this slender information in hand when the next al Qaeda plot moves toward execution.

As the United States fought the Afghanistan and Iraq wars, and continues to pursue al Qaeda groups in the Middle East and Africa, it captured al Qaeda laptops, cell phones, financial documents, and the other signs of modern high-tech life. This gave intelligence officers the information on dozens or hundreds of e-mail addresses, telephones, bank and credit account numbers, and residential and office addresses used by their network.[35] To exploit this, U.S. intelligence services must follow those leads as fast as possible, before the network of al Qaeda operatives can migrate to a new leader. An e-mail lead can disappear as fast as it takes someone to open a new e-mail account.

FISA, and the law enforcement mentality it embodies, creates several problems. FISA requires "probable cause" to believe that someone is an agent of a foreign power before one can get a warrant to collect phone calls and e-mails.[36] An al Qaeda leader could have a cell phone with 100 numbers in its memory, 10 of which are in the United States and thus require a warrant. Would a FISA judge have found probable cause to think the users of those 10 numbers are al Qaeda too? Probably not. Would our intelligence agencies even immediately know who was using those numbers at the time of captured al Qaeda leader's calls? The same is true of his e-mail, as to which it will not be immediately obvious what addresses are held by U.S. residents.

In our world of rapidly shifting e-mail addresses, multiple cell phone numbers, and internet communications, FISA imposes slow and cumbersome procedures on our intelligence and law enforcement officers.[37] These laborious checks are based on the assumption that we remain within the criminal justice system, and looking backward at crimes in order to conduct prosecutions, rather than within the national security system, which looks forward in order to prevent attacks on the American people.[38] FISA requires

---

[35] See, e.g., id. at 382.

[36] 50 U.S.C. § 1805(a)(3) (2000).

[37] See Americo R. Cinquegrana, The Walls (and Wires) Have Ears: The Background and First Ten Years of the Foreign Intelligence Surveillance Act of 1978 , 137 U. PA . L. REV . 793, 825 (1989), reasoning in 1989 that:

> FISA also must keep pace with the continuing explosion in communications technologies available both to law enforcement agencies and potential surveillance targets. FISA was drafted to take account of experience and technology developed between 1968 and 1978, but the decade since its passage has witnessed substantial technological changes that could require amendments to FISA in order to extend its privacy protections and to facilitate legitimate government interests that might otherwise be frustrated.

[38] See John Yoo, War by Other Means 71-74, 79-80 (2006) (noting that an artificial "Wall" in place for decades between information gathered for intelligence and information gathered for law enforcement purposes hindered the government's ability to piece together intelligence which could have stopped the 9/11 attacks).

a lengthy review process, in which special FBI and DOJ lawyers prepare an extensive package of facts and law to present to the FISC.[39] The Attorney General must personally sign the application, and another high-ranking national security officer, such as the President's National Security Advisor or the Director of the FBI, must certify that the information sought is for foreign intelligence.[40] Creating an existing database of numbers that can be quickly searched can allow the government to take advantage of captured al Qaeda numbers abroad, before the cells within the United States break their contacts.

A critic, however, might argue that billions of innocent calling records are not "relevant" to a terrorism investigation. Even if terrorist communications take place over the phone, that cannot justify the collection of all phone call records in the United States, the vast majority of which have nothing to do with the grounds for the search. The FISC rejected this argument because, to be useful, a database has to be broad enough to find terrorist calls. "Because known and unknown international terrorist operatives are using telephone communications, and because it is necessary to obtain the bulk collection of a telephone company's metadata to determine those connections between known and unknown international terrorist operatives as part of authorized investigations," the Court observed, "the production of the information sought meets the standard for relevance under Section 215."[41] Aggregating calling records into a database, the court found, was necessary to find the terrorist communications and the links between terrorists.[42] It may not even be possible to detect the links before such a database is created. If a database is not comprehensive, in other words, then the government will only be able to glimpse incomplete patterns of terrorist activity, if it can glimpse any at all.

Relevance is a slippery concept, but it cannot require that every piece of information obtained by subpoena must contain information related to guilt. Even when grand juries subpoena the business records or communications of a criminal suspect, it is likely that the large majority of the items will not have any relationship to the crime. Nonetheless, a grand jury may subpoena all of a suspect's financial records to find those that pertain to a criminal conspiracy. A different way to view NSA's telephone calling record program is that the "relevant" tangible "thing" is the database itself, rather than any individual calling record.

Of course, the NSA program differs from a subpoena to a financial institution for the records of a known criminal suspect. The amount of data collected by the NSA program are many orders of magnitude greater, and hence the percentage of directly involved communications much smaller. Also, unlike a regular subpoena, it is important to have as large a searchable database as possible, because the breadth will bring into the

[39] See 50 U.S.C. § 1804 (2000) (current version at 50 U.S.C.A. § 1804 (West 2006)).
[40] 50 U.S.C. 1804(a).
[41] In Re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things From, BR 13-109, at 18 (U.S. Foreign Intelligence Surveillance Court, Aug. 29, 2013), available at http://www.uscourts.gov/uscourts/courts/fisc/br13-09-primary-order.pdf.
[42] Id.

sharpest contrast the possible patterns of terrorist activity. On the other hand, the magnitude of harm that the government seeks to prevent exceeds by several orders that of regular crime and involves a foreign enemy, rather than persistent crime. The magnitude of the harm should be taken into account in judging relevance as well as the unprecedented difficulties of locating al Qaeda operatives disguised within the United States.

The NSA's second surveillance program, which targets internet communications involving foreigners, poses different legal challenges. But a careful review shows that it does not violate statutory or constitutional law, although the program's facts remain somewhat unclear. According to reports, in addition to the collection of telephone call metadata, the NSA also intercepts electronic communications—presumably e-mails—by foreigners outside the United States.[43] Apparently, this program also depends on the collection and storage of vast amounts of data, gained either by request from internet service providers (ISPs) or from the internet backbone networks themselves.[44] According to its own public description of the program in August 2013, the NSA generates "identifiers" of non-U.S. persons outside the country whom it is believed "possess, communicate, or are likely to receive foreign intelligence information authorized for collection under an approved certification."[45] The government uses these "identifiers," which take the form of e-mail addresses and phone numbers, to acquire selected communications.[46]

The NSA's program falls precisely within FISA as currently written. Congress specifically amended the statute, at first temporarily in 2007 and then permanently in 2008, to authorize this exact program.[47] It most recently renewed this authority, codified in Section 702 of FISA, in 2012.[48] Section 702 allows the government to target for surveillance a non-U.S. person reasonably believed to be outside the U.S. for up to one year. Congress specifically limited the reach of the statute in four ways. Surveillance may not:

1. intentionally target anyone known to be inside the United States
2. seek to reverse target a person believed to be in the United States through their contacts with individuals outside the U.S.
3. intentionally target any U.S. person
4. intentionally collect any communication where the sender and all receivers are known to be in the U.S.[49]

---

[43] NSA, The National Security Agency: Missions, Authorities, Oversight and Partnerships 4 (Aug. 9, 2013).
[44] Id.
[45] Id.
[46] Id.
[47] See Protect America Act of 2007, Pub. L. No. 110-55, 121 Stat. 552; FISA Amendments Act of 2008, Pub. L. No. 110-261, 122 Stat. 2436.
[48] FISA Amendments Act of 2012, codified at 50 U.S.C. 1881a.
[49] 50 U.S.C. 1881a(b).

These exceptions describe a specific category of communications that the government may collect: the communications of non-U.S. persons believed to be outside the U.S. It does not allow the surveillance of wholly domestic communications or those by U.S. persons anywhere in the world. Notice the important lacuna: the statute does not specify where the communications take place, only the locations of the persons engaged in communicating.

Congress's authorization of collection based only on the location of the sender and receiver is important because of the nature of internet communications. When a person sends an e-mail, the internet breaks the message up into packets, sends them through the most efficient network routes possible, and then reassembles them into the message at a point of reception. Depending on network efficiencies, the electronic communications of two people – even if they are in adjacent towns – might transverse any country where network backbones are located, such as the United States. Section 702 simply recognizes that a different set of surveillance authorities should not be triggered simply because part of a message between non-U.S. persons passes through the United States. For example, if a suspected terrorist in Pakistan were to send an email to an address of a person believed to be located in Afghanistan, the NSA could intercept the e-mail even if part or all of the message itself moved through communication networks located in the United States.

With internet communications, however, the government may not easily know the physical location or citizenship of the senders or receivers. An email addresses, such as yoo@law.berkeley.edu, does not obviously contain geographical location data. Berkeley might refer to a city in California, Australia, Canada, or the United Kingdom, or to the University of California at Berkeley. ISP-based emails, such as Gmail, Yahoo, or Hotmail, provide even less hint of a location. The government could look at metadata contained within the email messages themselves, or perhaps at the MAC addresses, which are unique to each computer, to attempt to determine location. But because of this lack of precision, it is inevitable that some unauthorized communications will be collected. As a result, Section 702 requires the FISC to approve the procedures used to develop targets and to minimize the collection of any communications by U.S. persons.[50] If the government seeks to intentionally collect the emails of U.S. persons or non-U.S. persons located in the U.S., it must still obtain a FISC court order.[51]

The second NSA surveillance program fits cleanly within statutory authorization because Congress amended FISA precisely to fit the program. To be sure, there have been disagreements between the FISC and the NSA over the exact implementation of the program in a manner consistent with Section 702. Examination of the FISC opinions made public, however, indicate that these contests involve minimization procedures where the NSA has intercepted a relatively small number of domestic communications or emails by U.S. persons. In October 2011, for example, the FISC criticized an NSA

[50] 50 U.S.C. § 1881a(g).
[51] 50 U.S.C. 1804.

technique of collecting emails from "upstream" sources – i.e., from the internet backbone itself rather than from ISPs – because it swept in several thousand domestic e-mails out of tens of millions of foreign emails.[52] The FISC's opinion did not terminate the program, but instead led the NSA to modify its minimization procedures in order to avoid collection of the domestic e-mails.[53] One month later, the FISC approved the new minimization procedures and the collection program continued.[54] These declassified FISC opinions make clear that judicial resistance to the NSA's program comes not from the legal authority for the electronic surveillance, but from second order concerns over implementation. Concerns about the legality over the program cannot arise over FISA or other statutes, but over the Constitution.

III.

Even if Congress and the President have sufficient power under statutory law to carry out the NSA programs, they may still violate the Constitution. A government decision may satisfy the structural provisions of the Constitution—such as the separation of powers and federalism—yet still run afoul of the Bill of Rights. This Part measures the two NSA programs against the primary individual right at stake, the Fourth Amendment's protection against unreasonable searches and seizures. It concludes that both the telephone metadata and foreign e-mail collection programs, as currently described by the Obama administration, do not violate the Fourth Amendment.

NSA's first program, which collects metadata of domestic phone calls, poses the least constitutional difficulties. Under existing judicial doctrine, individuals have Fourth Amendment rights in the content of communications, but not in their addressing information.[55] However, privacy does not extend to the writing on the outside of envelopes deposited in the mail because the sender has voluntarily revealed the addresses to the post office for delivery.[56] An identical principle applies to telecommunications. In *Smith v. Maryland*, the Supreme Court found calling information, such as the phone number dialed, beyond Fourth Amendment protection because the consumer had voluntarily turned over the information to a third party—namely, the phone company for

[52] FISA Court Memorandum Opinion and Order of Oct. 3, 2011, available at http://www.odni.gov/files/documents/October%202011%20Bates%20Opinion%20and%20Order%20Part%201.pdf.
[53] Id.
[54] FISA Court Memorandum Opinion and Order of Nov. 30, 2011, available at http://www.odni.gov/files/documents/November%202011%20Bates%20Opinion%20and%20Order%20Part%201.pdf.
[55] Smith v. Maryland, 442 U.S. 735, 744-45 (1979); United States v. Miller, 425 U.S. 435, 443 (1976).
[56] See, e.g., Katz v. United States, 389 U.S. 347, 351 (1967) (holding that "[w]hat a person knowingly exposes to the public . . . is not a subject of Fourth Amendment Protection.").

connection and billing purposes.[57] In the rubric of *Katz v. United States*, no one can have an expectation of privacy in records that they have handed over to someone else.[58]

In recent cases, however, the Court has turned a skeptical eye toward new search technologies. In *Kyllo v. United States*, for example, the Court held that thermal imaging of homes qualified as a search under the Fourth Amendment, even though the police used device from a public street.[59] In *United States v. Jones*, the Court found that the Fourth Amendment required a warrant for the placement of a global positioning service tracker on a car.[60] These cases depend on the means by which the government conducts a search in a place protected by the Fourth Amendment. In *Kyllo*, the Court believed that thermal imaging verged on a physical search of a home, while *Jones* involved physical intrusion into a private car. Neither holding calls into doubt the loss of Fourth Amendment rights when an individual voluntarily hands over information to a third party. In other words, the information sought by the NSA programs would enjoy constitutional protections if it remained within the home or personal computing devices. But they lose their status when an individual reveals them to another. As a result, the Constitution does not require a warrant for a pen register because no electronic interception or surveillance of the content of the calls has occurred.

Meanwhile, the data collected is potentially of enormous use in frustrating al Qaeda plots. If U.S. agents are pointed to members of an al Qaeda sleeper cell by a domestic phone number found in a captured al Qaeda leader's cell phone, call pattern analysis would allow the NSA to quickly determine the extent of the network and its activities. The NSA, for example, could track the sleeper cell as it periodically changed phone numbers. This could give a quick, initial database-generated glimpse of the possible size and activity level of the cell in an environment where time is of the essence. A critic might respond that there is a difference between a pen register that captures the phone numbers called by a single person and a database that captures all of the phone numbers called by everyone in the United States. The Supreme Court, however, has never held that obtaining billing records would somehow violate privacy merely because of a large number of such records.

A different Fourth Amendment issue applies to the second NSA program, which intercepts emails between foreigners abroad. As the Supreme Court has observed, the Fourth Amendment does not provide rights outside the United States except to citizens or those with sufficient connections to the nation, such as permanent resident aliens. In *United States v. Verdugo-Urquidez*, the Court held that a non-U.S. person could not claim any constitutional rights to bar his capture outside the United States.[61] A critic might respond that the Bill of Rights limits the powers of the government regardless of the citizenship of the individual involved. Tellingly, the Court rejected this argument because

[57] Id.
[58] Katz, 389 U.S. at 358 n.23
[59] 533 U.S. 27 (2001).
[60] 565 U.S. ___, 132 S.Ct. 945 (2012)/
[61] Verdugo-Urquidez, 494 U.S. 259, 273 (1990).

it would render impossible the conduct of war against foreign enemies.[62] If all foreigners held Fourth Amendment rights, the Court reasoned, the U.S would be unable to use force against them in wartime without a warrant or a determination of constitutional reasonableness after the fact.[63] Such a rule, the Court reasoned, had never prevailed in American history.[64] So long as the second NSA program collects foreign emails between non-U.S. persons, the Fourth Amendment is not implicated.[65]

There is one critical fact about the e-mail intercept program, however, that might trigger the Fourth Amendment. Passage of e-mail packets through switches or network backbones located within the territorial United States might create enough of a nexus with the United States to garner constitutional protections. A court might analogize the legal status of e-mails to an air flight that takes off from Canada and lands in Mexico – while the plane flies over the United States, it falls subject to the jurisdiction of the United States.

There are several reasons, however, that this analogy fails. First, packets are not the message themselves, but are pieces of them that are broken apart and reassembled. The message itself is not in a completed form except when it is first written or when it is later reassembled. At those points in time, when the message is actually a unified whole, it is located outside the United States.

Second, because of the presence of much of the internet backbone in the United States, finding that any packet that transverses the United States triggers the Bill of Rights would effectively extend constitutional status to all email communications in the world due to central importance of the U.S. to the operation of the internet. If everyone in the world has a constitutional right, then the Constitution has lost its meaning as a framework of government for a single community:"We the People" of the United States.[66] This is a result that the Court in *Verdugo-Urquidez* expressly sought to avoid.

Third, non-U.S. persons communicating outside the U.S. could not possibly have an expectation of privacy under the Fourth Amendment. To be sure, they might think their messages are private because of the difficulty of intercepting internet communications. But they could not think they had any expectation of privacy cognizable under the U.S. Constitution when they were not located within the United States and had no other connections to the nation. Non-U.S. persons outside the territorial U.S. do not have enough connections with the U.S. to benefit from its laws and constitutional protections.

---

[62] Id. at 273-74.
[63] Id.
[64] Id. at 274-275.
[65] Id. at 275.
[66] For a broader explanation of the relationship of the Constitution's guiding principle of popular sovereignty with national security and foreign affairs, see Julian Ku & John Yoo, Taming Globalization: International Law, the U.S. Constitution, and the New World Order (2012).

Even if constitutional privacy interests were thought to extend to telephone metadata or foreign emails, the Fourth Amendment's warrant requirement would still not apply because the NSA searches seek to prevent military attacks, not garden-variety criminal activity.[67] As observed earlier, every lower court to examine the question has found that when the government conducts a search of a foreign power or its agents, it need not meet the requirements that apply to criminal law enforcement. Though admittedly, the Supreme Court has never held on the question, it has suggested in dicta that roadblocks and dragnets to stop a terrorist bombing in an American city would not need to meet the warrant requirement's demand for individualized suspicion.[68]

This approach is fully consistent with the Supreme Court's recent Fourth Amendment cases. Not all searches require a warrant. Rather, as the Court found in a 1995 case upholding random drug testing of high school athletes, "[a]s the text of the Fourth Amendment indicates, the ultimate measure of the constitutionality of a governmental search is 'reasonableness.'" [69] When a passenger enters an airport, government employees search his belongings and subject him to an X-ray—undoubtedly a search—without a warrant. When travelers enter the country, customs and immigration officials can search their baggage and sometimes their person without a warrant.[70] Of course, when law enforcement undertakes a search to discover evidence of criminal wrongdoing, reasonableness generally requires a judicial warrant. But when the government's conduct is not focused on law enforcement, a warrant is unnecessary. A warrantless search can be constitutional, the Court has said, "when special needs, beyond the normal need for law enforcement, make the warrant and probable-cause requirement impracticable."[71]

A search must be "reasonable" under the circumstances. What does "reasonable" mean? The Court has upheld warrantless searches to reduce deaths on the nation's highways, maintain safety among railway workers, and ensure that government officials were not using drugs.[72] In these cases, the "importance of the governmental interests"

---

[67] This conclusion is supported by the Supreme Court's recent "special needs" cases, which allow reasonable, warrantless searches for government needs that go beyond regular law enforcement. See Vernonia School Dist. 47J v. Acton, 515 U.S. 646, 653, 115 S.Ct. 2386, 2391, 132 L.Ed.2d 564 (1995) (random drug-testing of student athletes); Michigan Dep't of State Police v. Sitz, 496 U.S. 444 (1990) (stopping drunk drivers); United States v. Martinez-Fuerte, 428 U.S. 543 (1976) (border control checkpoints).

[68] City of Indianapolis v. Edmond, 531 U.S. 32, 44 (2000).

[69] Vernonia School Dist. 47J v. Acton, 515 U.S. 646, 652 (1995).

[70] See, e.g., U.S. v. Montoya de Hernandez, 473 U.S. 531, 538 (1985).

[71] Vernonia, 515 U.S. at 653 (quoting Griffin v. Wisconsin, 483 U.S. 868, 873 (1987).

[72] See, e.g., Pennsylvania v. Labron, 518 U.S. 938 (1996) (per curiam) (automobile searches); Acton (drug testing of athletes); Michigan v. Dept. of State Police v. Sitz, 496 U.S. 444 (1990) (drunk driver checkpoints); Skinner v. Railway Labor Executives' Ass'n., 489 U.S. 602 (1989) (drug testing railroad personnel); Treasury Employees v. Von Raab, 489 U.S. 656 (1989) (drug testing federal customs officers); United States v.

outweighed the "nature and quality of the intrusion on the individual's Fourth Amendment interests."[73] It is hard to imagine that any of these situations are more important than protecting the nation from a direct foreign attack in wartime. "It is 'obvious and unarguable,'" the Supreme Court has observed several times, "that no governmental interest is more compelling than the security of the Nation."[74] It is the duty of the President to respond to attacks on the territory and people of the United States. Congress confirmed the President's authority to use force after 9/11. The extraordinary circumstances of war require that the government seek specific information relevant to possible attacks on Americans, sometimes in situations where a warrant is not practical.[75]

Before the 9/11 attacks, the Supreme Court observed that the Fourth Amendment's warrant requirement would probably not apply to the special circumstances created by a potential terrorist attack. "[T]he Fourth Amendment would almost certainly permit an appropriately tailored roadblock set up to thwart an imminent terrorist attack or to catch a dangerous criminal who is likely to flee by way of a particular route."[76] To be sure, this 2000 case challenged the constitutionality of a highway checkpoint program that searched cars for illegal drugs, not a search for terrorists. And in this case the Court found that the checkpoints violated the Fourth Amendment protection against search and seizure because the police were searching for drugs for the purpose of "crime control" and "the ordinary enterprise of investigating crimes."[77] But the Court was still observing that some warrantless searches were acceptable in the emergency situation of a possible terrorist attack, in which the "need for such measures to ensure public safety can be particularly acute."[78]

If national security searches do not require a warrant, it might be asked why FISA is even necessary. FISA offers the executive branch a deal. If a President complies with the process of obtaining a FISA warrant, courts will likely agree that the search was reasonable and will admit its fruits as evidence in a criminal case. FISA does not create the power to authorize national security searches. Rather, it describes a safe harbor that deems searches obtained with a warrant reasonable under the Fourth Amendment. If a President proceeds with a search under his own authority rather than under FISA or under ordinary criminal procedure, he takes his chances. A court might refuse to admit evidence

---

Place, 462 U.S. 696 (1983) (baggage search); Terry v. Ohio, 392 U.S. 1 (1968) (temporary stop and search).

[73] See Tennessee v. Garner, 471 U.S. 1, 8 (1985).

[74] Haig v. Agee, 453 U.S. 280, 307 (1981).

[75] The courts have observed that even the use of deadly force is reasonable under the Fourth Amendment if used in self-defense or to protect others. Here, the right to self-defense is not that of an individual, but that of the nation and of its citizens. Cf. In re Neagle, 135 U.S. 1 (1890); The Prize Cases, 67 U.S. (2 Black) 635 (1862). If the government's heightened interest in self-defense justifies the use of deadly force, then it certainly would also justify warrantless searches.

[76] City of Indianapolis, 531 U.S. at 44.

[77] Id. at 44.

[78] Id. at 47-48.

in any future proceeding that had been obtained without a warrant, or even allow the target to sue the government for damages.[79] Then again, it might not.

FISA ultimately cannot limit the President's powers to protect national security through surveillance if those powers stem from his unique Article II responsibilities. Intercepting enemy communications has long been part of waging war; indeed, it is critical to the successful use of force. Gathering intelligence has long been understood as a legitimate aspect of conducting war.[80] The U.S. military cannot attack or defend to good effect unless it knows where to aim. America has a long history of conducting intelligence operations to obtain information on the enemy. General Washington used spies extensively during the Revolutionary War, and as president established a secret fund for spying that existed until the creation of the CIA.[81] President Lincoln personally hired spies during the Civil War, a practice the Supreme Court upheld.[82] In both World Wars I and II, Presidents ordered the interception of electronic communications leaving the United States.[83] Some of America's greatest wartime intelligence successes have involved SIGINT, most notably the breaking of Japanese diplomatic and naval codes during World War II, which allowed the U.S. Navy to anticipate the attack on Midway Island.[84] SIGINT is even more important in this war than in those of the last century. Al Qaeda has launched a variety of efforts to attack the United States, and it intends to continue them. The primary way to stop those attacks is to find and stop al Qaeda operatives who have infiltrated the United States. The best way to find them is to intercept their electronic communications entering or leaving the country.

The need for executive authority over electronic intelligence gathering becomes apparent when we consider the facts of the war against al Qaeda. In the hours and days after 9/11, members of the government thought that al Qaeda would try to crash other airliners or use a weapon of mass destruction in a major East Coast city, probably Washington, D.C. Combat air patrols began flying above New York and Washington.

---

[79] Cf. Akhil Amar, The Constitution and Criminal Procedure: First Principles 1-45 (1998).

[80] In the 1907 Hague Regulations, one of the first treaties on the laws of war, the leading military powers agreed that "the employment of measures necessary for obtaining information about the enemy and the country is considered permissible." Interception of electronic communications is known as SIGINT, or signals intelligence, as opposed to HUMINT, or human intelligence. Writers on the laws of war have recognized that interception of an enemy's communications is a legitimate tool of war. According to one recognized authority, nations at war can gather intelligence using air and ground reconnaissance and observation, "interception of enemy messages, wireless and other," capturing documents, and interrogating prisoners. Morris Greenspan, The Modern Law of Land Warfare 326 (1959).

[81] Halperin v. CIA, 629 F.2d 144, 158 (D.C. Cir. 1980).

[82] Totten v. United States, 92 U.S. 105 (1876).

[83] Exec. Order No. 2604 (Apr. 28, 1917) (World War I order); Exec. Order No. 8985 (Dec. 19, 1941) (World War II order).

[84] Christopher Andrew, For the President's Eyes Only 124-25 (1995).

Suppose a plane was hijacked and would not respond to air traffic controllers. In order to protect the nation from attack, it would be reasonable for U.S. anti-terrorism personnel to intercept any radio or cell phone calls to or from the airliner, in order to discover the hijackers' intentions, what was happening on the plane, and ultimately whether it would be necessary for the fighters to shoot down the plane. Or suppose the government had to put up a net to intercept all cellular phone calls in a city because it was searching for a terrorist cell which had yet to launch an attack. Under such circumstances, FISA should not control whether the President has the executive authority to monitor any radio or cell phone calls to or from the airliner; after all, the purpose is not to arrest and gather evidence for trial, but to prevent the nation from attack. Indeed, because the United States is in a state of war, the military can intercept the communications of the plane to see if it poses a threat, and target the enemy if necessary. This authority is not only within the President's executive powers, but it also comports with the principle of reasonableness that guides the Fourth Amendment.

As Commander-in-Chief, the President has the constitutional power and the responsibility to wage war in response to a direct attack against the United States. In the Civil War, President Lincoln undertook several actions—raised an army, withdrew money from the treasury, launched a blockade—on his own authority in response to the Confederate attack on Fort Sumter, moves that Congress and the Supreme Court later approved.[85] During World War II, the Supreme Court similarly recognized that once war began, the President's authority as Commander-in-Chief and Chief Executive gave him the tools necessary to effectively wage war.[86] In the wake of the September 11 attacks, Congress agreed that "the President has authority under the Constitution to take action to deter and prevent acts of international terrorism against the United States," which recognizes the President's authority to use force to respond to al Qaeda, and any powers necessary and proper to that end.[87]

Even legal scholars who argue against this historical practice concede that once the United States has been attacked, the President can respond immediately with force. The ability to collect intelligence is intrinsic to the use of military force. It is inconceivable that the Constitution would vest in the President the powers of Commander-in-Chief and Chief Executive, give him the responsibility to protect the nation from attack, but then disable him from gathering intelligence to use the military most effectively to defeat the enemy. Every evidence of the Framers' understanding of the Constitution is that the government would have every ability to meet a foreign danger. As James Madison wrote in *The Federalist*, "security against foreign danger is one of the

---

[85] The Prize Cases, 67 U.S. 635, 670 (1863). For a more detailed discussion, see John Yoo, Crisis and Command: Executive Power from George Washington to George W. Bush (2010).

[86] The President has the power "to direct the performance of those functions which may constitutionally be performed by the military arm of the nation in time of war," and to issue military commands using the powers to conduct war "to repel and defeat the enemy." Ex Parte Quirin, 317 U.S. 1, 28 (1942).

[87] Authorization for the Use of Military Force, Pub. L. 107-40 (Sept. 18, 2001).

primitive objects of civil society."[88] Therefore, the "powers requisite for attaining it must be effectually confided to the federal councils." After World War II, the Supreme Court declared, "this grant of war power includes all that is necessary and proper for carrying these powers into execution."[89] Covert operations and electronic surveillance are clearly part of this authority.

During the writing of the Constitution, some Framers believed that the President alone should manage intelligence because only he could keep secrets.[90] Several Supreme Court cases have recognized that the President's role as Commander-in-Chief and the sole organ of the nation in its foreign relations must include the power to collect intelligence.[91] These authorities agree that intelligence rests with the President because its structure allows it to act with unity, secrecy, and speed.

Presidents have long ordered electronic surveillance without any judicial or congressional participation. More than a year before the Pearl Harbor attacks, but with war clearly looming with the Axis powers, President Franklin Roosevelt authorized the FBI to intercept any communications, whether wholly inside the country or international, of persons "suspected of subversive activities against the Government of the United States, including suspected spies."[92] FDR was concerned that "fifth columns" could wreak havoc with the war effort. "It is too late to do anything about it after sabotage, assassinations and 'fifth column' activities are completed," FDR wrote in his order. FDR ordered the surveillance even though a federal law at the time prohibited electronic surveillance without a warrant.[93] Presidents continued to monitor the communications of national security threats on their own authority, even in peacetime.[94] If Presidents in times of peace could order surveillance of spies and terrorists, executive authority is only the greater now, as hostilities continue against al Qaeda. This is a view that Justice Departments have not just held under Presidents George W. Bush or Barack Obama. The

---

[88] Federalist No. 41 (James Madison).
[89] Johnson v. Eisentrager, 339 U.S. 763, 788 (1950).
[90] Federalist No. 64, at 435 (Jacob E. Cooke ed. 1961) (John Jay).
[91] See, e.g., United States v. Curtiss-Wright Export Corp., 299 U.S. 304 (1936); Chicago & S. Air Lines v. Waterman S.S. Corp., 333 U.S. 103, 111 (1948). In a post-Civil War case, recently re-affirmed, the Court ruled that President Lincoln had the constitutional authority to engage in espionage. The President "was undoubtedly authorized during the war, as commander-in-chief . . . to employ secret agents to enter the rebel lines and obtain information respecting the strength, resources, and movements of the enemy." Totten v. United States, 92 U.S. 105, 106 (1876). On Totten's continuing vitality, see Tenet v. Doe, 544 U.S. 1, 8-11 (2005).
[92] Reprinted in Appendix A, United States v. United States District Court, 444 F.2d 651, 669-70 (6th Cir. 1971).
[93] See Nardone v. United States, 302 U.S. 379 (1937) (interpreting Section 605 of Federal Communications Act of 1934 to prohibit interception of telephone calls).
[94] Foreign Intelligence Surveillance Act of 1978: Hearings on H.R. 5764, H.R. 9745, H.R. 7308, and H.R. 5632 Before the Subcomm. on Legislation of the House Comm. on Intelligence, 95th Cong., 2d Sess.15 (1978) (Statement of Attorney General Griffin Bell).

Clinton Justice Department held a similar view of the executive branch's authority to conduct surveillance outside the FISA framework.[95]

Courts have never opposed a President's authority to engage in warrantless electronic surveillance to protect national security. When the Supreme Court first considered this question in 1972, it held that the Fourth Amendment required a judicial warrant if a President wanted to conduct surveillance of a purely domestic group, but it refused to address surveillance of foreign threats to national security.[96] In the years since, every federal appeals court, including the FISA Appeals Court, to address the question has "held that the President did have inherent authority to conduct warrantless searches to obtain foreign intelligence information."[97] The FISA Appeals Court did not even feel that it was worth much discussion. It took the President's power to do so "for granted," and observed that "FISA could not encroach on the President's constitutional power."[98]

Congress also implicitly authorized the President to carry out electronic surveillance to prevent further attacks on the United States. Congress's September 18, 2001 Authorization to Use Military Force (AUMF) is sweeping; it has no limitation on time or place—only that the President pursue al Qaeda.[99] Although the President did not need, as a constitutional matter, Congress's permission to pursue and attack al Qaeda after the attacks on New York City and the Pentagon, its passage shows that the President and Congress fully agreed that military action would be appropriate. Congress's approval of the killing and capture of al Qaeda must obviously included the tools to locate them in the first place.

A choice between FISA or his constitutional authority gives the President the discretion to use the best method to protect the United States, whether through the military or by relying on law enforcement. It also means warrantless surveillance will not be introduced into the criminal justice system; the judiciary is only needed to enforce this legal distinction. Presidents could alleviate concern about the NSA programs by publicly declaring that no evidence generated by them will be used in a criminal case. Although

---

[95] Most notably, Clinton Deputy Attorney General Jamie Gorelick testified before Congress that the Justice Department could carry out physical searches for foreign intelligence purposes, even though FISA at the time did not provide for them. Amending the Foreign Intelligence Surveillance Act: Hearings Before the House Permanent Select Comm. on Intelligence, 103d Cong. 2d Sess. 61 (1994). Clinton's OLC even issued a legal opinion that the President could order the sharing of electronic surveillance gathered through criminal wiretaps between the Justice Department and intelligence agencies, even though this was prohibited by statute. Sharing Title III Electronic Surveillance Material with the Intelligence Community, OLC Prelim. Print, 2000 WL 33716983 (Oct. 17, 2000).

[96] United States v. United States District Court, 407 U.S. 297 (1972).

[97] In re Sealed Case, 310 F.3d 717, 742 (For. Intel. Surv. Ct. Rev. 2002).

[98] Id.

[99] Pub. L. No. 107-40, 115 Stat. 224 (Sept. 18, 2001).

FISA cannot supercede the President's constitutional authority, it can provide a more stable system for the domestic collection of foreign intelligence, such as the NSA's collection of phone call metadata and foreign e-mails.

## Conclusions

The real problem with FISA, and even the Patriot Act, as they existed before the 2008 Amendments, is that they remained rooted in a law enforcement approach to electronic surveillance. They tied the government's counter-terrorism efforts to individualized suspicion. Searches and wiretaps had to target a specific individual already believed to be involved in harmful activity. But detecting al Qaeda members who have no previous criminal record in the United States, and who are undeterred by the possibility of criminal sanctions, requires the use of more sweeping methods.

To successfully prevent attacks, the government has to devote surveillance resources where there is a reasonable chance that terrorists will appear, or communicate, even if their specific identities remain unknown. What if the government knew that there was a fifty percent chance that terrorists would use a certain communications pipeline, such as e-mails provided by a popular Pakistani ISP, but that most of the communications on that channel would not be linked to terrorism? An approach based on individualized suspicion would prevent computers from searching through that channel for the keywords or names that might suggest terrorist communications, because there are no specific al Qaeda suspects, and thus no probable cause. Rather than individualized suspicion, searching for terrorists depends on playing the probabilities, just as roadblocks or airport screenings do. The private owner of any website has detailed access to information about the individuals who visit the site that he can exploit for his own commercial purposes, such as selling lists of names to spammers, or gathering market data on individuals or groups. Is the government's effort to find violent terrorists a less legitimate use of such data?

Individualized suspicion dictates the focus of law enforcement, but war demands that our armed forces defend the country with a broader perspective. Armies do not meet a "probable cause" requirement when they attack a position or fire on enemy troops or intercept enemy communications on a frequency. In the criminal justice system the purpose is to hold a specific person responsible for a discrete crime that has already happened. It does not make sense when the purpose of intelligence is to take action, such as killing or capturing members of the enemy, to prevent future harm to the nation from a foreign threat.

FISA should be regarded as a safe harbor that allows the fruits of an authorized search to be used for prosecution. Using FISA sacrifices speed and breadth of information in favor of individualized suspicion, but it provides a path for using evidence in a civilian criminal prosecution. If the President chooses to rely on his constitutional authority alone to conduct warrantless searches, then he should generally only use the information for military purposes. The primary objective of the NSA program is to "detect and prevent" possible al Qaeda attacks on the United States, whether another

attack like September 11; a bomb in apartment buildings, bridges, or transportation hubs such as airports; or a nuclear, biological, or chemical attack. These are not hypotheticals; they are all al Qaeda plots, some of which U.S. intelligence and law enforcement agencies have already stopped. A President will want to use information gathered by the NSA to deploy military, intelligence, and law enforcement personnel to stop the next attack. The price to pay for speed, however, is foregoing any future criminal prosecution. If the President wants to use the NSA to engage in warrantless searches, he cannot use its fruits in an ordinary criminal prosecution.

Al Qaeda has launched a variety of efforts to attack the United States, and it intends to continue them. The primary way to stop those attacks is to find and stop al Qaeda operatives, and the best way to find them is to intercept their electronic communications. Properly understood, the Constitution does not subject the government to unreasonable burdens in carrying out its highest duty of protecting the nation from attack.

Preliminary Draft – Please Do Not Cite Without Permission
To be Published in *I/S: A Journal of Law and Policy for the Information Society*
9 ISJLP ___ (2014).
http://www.is-journal.org

# Membership Lists, Metadata, and Freedom of Association's Specificity Requirement

Katherine J. Strandburg
New York University School of Law

We now know that the National Security Agency (NSA) routinely collects telephone call traffic data ("telephony metadata") from nearly all calls made to or from United States telecommunications carriers. Its purpose is "to identify otherwise unknown connections between telephone numbers associated with known or suspected terrorists and other telephone numbers, and to analyze those connections in a way that can help identify terrorist operatives or networks" by using aggregated data to follow "chains of communications" between suspected terrorists and other individuals.[1] Since 2006, this comprehensive metadata acquisition has been conducted in reliance on two sources of legal authority: 1) "Section 215 orders" issued secretly by the Foreign Intelligence Surveillance Court (FISC) under the auspices of the Foreign Intelligence Surveillance Act (FISA) and 2) the Supreme Court's ruling in *Smith v. Maryland*[2] that there is no Fourth Amendment protection for dialed telephone numbers, which are exposed to telecommunications providers in the ordinary course of business.

In a 2008 article,[3] I argued that metadata surveillance of this sort is unconstitutional unless conducted in compliance with First Amendment freedom of association guarantees. This article expands on that analysis, arguing that the right to freedom of association imposes specificity requirements on government collection of membership lists and related associational information. The NSA's metadata surveillance program does not comply with these specificity requirements.

[1] Administration White Paper at 13.
[2] 4442 U.S. 735 (1979)
[3] Strandburg, Relational Surveillance. See also Solove, First Amendment Criminal Procedure.

Part I reviews freedom of association case law, particularly as it pertains to compelled disclosure of associational information. It argues that the right to freedom of association imposes specificity requirements on legal tools for acquiring associational information. It then discusses the "good faith investigation" standard, which the government invokes to justify the NSA's comprehensive metadata surveillance, arguing that, when investigations aim to acquire associational information, "good faith" does not mean merely "good intentions," but must incorporate specificity requirements. Part II discusses the NSA's telephony metadata surveillance program, focusing on the ways in which social network analysis might be used to identify possible members of terrorist groups. Part III evaluates the NSA's telephony metadata surveillance in light of freedom of association's specificity requirements. Part IV discusses the challenges to freedom of association presented by the digitally intermediated technosocial milieu and considers how freedom of association might be protected in a "big data" world.

## I. Freedom of Association's Specificity Requirements

### A. Freedom of Association Protection of Associational Information

The Supreme Court has emphasized that "'implicit in the right to engage in activities protected by the First Amendment' is 'a corresponding right to associate with others in pursuit of a wide variety of political, social, economic, educational, religious, and cultural ends.' This right is crucial in preventing the majority from imposing its views on groups that would rather express other, perhaps unpopular, ideas." [4] This Article focuses on "expressive association,"[5] in which individuals come together to express themselves "public[ly] or private[ly]."[6] Protected expressive association is broadly defined: "[A]ssociations do not have to associate for the 'purpose' of disseminating a certain message in order to be entitled to the protections of the First Amendment. An association must merely engage in expressive

[4] Boy Scouts of America v. Dale, 530 U.S. 640, 657-58 (2000). (quoting and citing Roberts v. United States Jaycees, 468 U.S. 609 (1984) for the proposition that "protection of the right to expressive association is "especially important in preserving political and cultural diversity and in shielding dissident expression from suppression by the majority").
[5] *Id.* at 653.
[6] Id.

activity that could be impaired in order to be entitled to protection."[7] Freedom of association protection is not limited to unpopular associations[8] and is available to groups with mixed purposes.[9]

Freedom of association cases follow two major threads: those concerned with government actions that compel, prohibit or otherwise directly burden association and those concerned with government attempts to obtain information about association membership. Both threads apply strict, or "exacting," scrutiny, requiring that government actions that burden freedom of association be "adopted to serve compelling state interests, unrelated to the suppression of ideas that cannot be achieved through means significantly less restrictive of associational freedoms."[10]

In a seminal case, the Court quashed Alabama's request for an NAACP membership list, comparing it to a requirement that members wear identifying arm-bands:

> This Court has recognized the vital relationship between freedom to associate and privacy in one's associations. When referring to the varied forms of governmental action which might interfere with freedom of assembly, it said []: "A requirement that adherents of particular religious faiths or political parties wear identifying arm-bands, for example, is obviously of this nature." Compelled disclosure of membership in an organization engaged in advocacy of particular beliefs is of the same order. Inviolability of privacy in group association may in many circumstances be indispensable to preservation of freedom of association, particularly where a group espouses dissident beliefs.[11]

To justify burdening the right to freedom of association by compelling disclosure of association membership, the "subordinating interest of the State must be compelling."[12] If the government

---

[7] *Id.* at 654.

[8] This is evident from the Court's ruling in *Boy Scouts*, which perhaps could not have involved a more popular organization. See also, e.g., Britt v. Superior Court, 574 P.2d 766 (Cal. 1978).

[9] See, e.g., In re Grand Jury Proceeding, 842 F.2d 1229 (11th Cir. 1988); In re Motor Fuel Temperature Sales Practices Litigation, 641 F.3d 470 (10th Cir. 2011).

[10] Roberts v. United States Jaycees, 468 U.S. 609, 623 (1984); Boy Scouts of Amer. v. Dale, 530 U.S. 640 (2000) (applying Roberts standard and refusing to apply O'Brien intermediate scrutiny standard); Knox v. SEIU, 132 S. Ct. 2277 (2012) (applying Roberts standard).

[11] *NAACP v. Alabama*, 357 U.S. 449 (1958). See also Bates v. City of Little Rock, 361 U.S. 516; Gibson v. Florida Legislative Investigation Committee, 372 U.S. 539 (1963).

[12] NAACP v. Alabama, 357 U.S. 449, 462 (1958) (state must demonstrate interest in obtaining membership lists that is "compelling"). See also, e.g., Bates v. City of Little Rock, 361 U.S. 516 (1960) (same); Gibson v. Florida Legislative Investigation Comm., 372 U.S. 539 (1963) ("regardless of the label applied, be it "nexus," "foundation," or whatever – [] it is an essential prerequisite to the validity of an investigation which intrudes into the area of constitutionally protected rights of speech, press, association and petition that the State convincingly show a substantial relation between the information sought and a subject of overriding and compelling state interest."); Buckley v. Valeo, 424 U.S. 1 (1976) ("We long have recognized

articulates a compelling interest, the "breadth of legislative abridgment must be viewed in the light of less drastic means for achieving the same basic purpose."[13]

Courts have subjected compelled disclosure of associational information to exacting scrutiny in cases involving statutes,[14] grand jury and administrative subpoenas,[15] and civil discovery.[16] For example, in assessing a grand jury subpoena for testimony about membership information, the Second Circuit required 1) compelling state interests able to survive "exacting scrutiny as to whether they are "sufficiently important to outweigh the possibility of infringement;" 2) a "substantial relation between the governmental interest and the information required to be disclosed;" and 3) that "justifiable governmental goals may not be achieved by unduly broad means having an unnecessary impact on protected rights of speech, press, or association."[17] When freedom of association interests are at stake, the usual relevance standard applied to subpoenas is insufficient.[18]

---

that significant encroachments on First Amendment rights of the sort that compelled disclosure imposes cannot be justified by a mere showing of some legitimate governmental interest.")

[13] NAACP v. Alabama.

[14] See, e.g., NAACP v. Alabama; Shelton v. Tucker; Paton v. La Prade 469 F. Supp. 773 (DNJ 1978).

[15] See, e.g., Gibson v. Florida Legislative Investigation Comm. (1963); In re Grand Jury Proceedings, 776 F.2d 1099 (2d. Cir. 1985); In re Grand Jury Proceeding, 842 F.2d 1229 (11th Cir. 1988) (grand jury subpoena for membership records of tax protest organization); Brock v. Local 375 (9th Cir.); US v. Citizens State Bank (8th Cir. 1980); Local 1814, Int'l Longshoremen's Ass'n v. Waterfront Comm'n (2d Cir.); In re Grand Jury Subpoena (10th Cir. 1983); EEOC v. Univ. of Penn. (3rd Cir. 1988); St. German of Alaska v. USA (2d Cir. 1988); In re Grand Jury Subpoenas to Locals 17, 135, 257, and 608, 528 N.E.2d 1195 (N.Y. 1988) (grand jury subpoena for union membership records).

[16] See, e.g., See, e.g., Britt v. Superior Ct. (Cal. 1978); Etsi Pipeline Project v. Burlington Northern (DDC 1987); Grandbouche v. Clancy (825 F.2d 1463, 1466 (10th Cir. 1987); New York State Nat'l Org. for Women v. Terry (2d Cir. 1989); Snedigar v. Hodderson (Wash. 1990); Perry v. Schwarzenegger (9th Cir. 2010).

[17] In re Grand Jury Proceedings, 776 F.2d 1099 (2d. Cir. 1985).

[18] See, e.g. FEC v. The Larouche Campaign, 817 F.2d 233 (2d Cir. 1987) ("However, as the court below recognized, different considerations come into play when a case, as here, implicates first amendment concerns. In that circumstance the usual deference to the administration agency is not appropriate, and protection of the constitutional liberties of the target of the subpoena calls for a more exacting scrutiny of the justification offered by the agency.") See also Perry v. Schwarzenegger ("Importantly, the party seeking the discovery must show that the information sought is highly relevant to the claims or defenses in the litigation -- a more demanding standard of relevance than that under *Federal Rule of Civil Procedure 26(b)(1)*. The request must also be carefully tailored to avoid unnecessary interference with protected activities, and the information must be otherwise unavailable." ); EEOC v. Univ. Penn.

Disclosure mandates directed to third parties, such as banks, usually must meet the same standard of scrutiny.[19] In *In re First National Bank*, for example, the court distinguished the Supreme Court's holding in *U.S. v. Miller* that there was no Fourth Amendment expectation of privacy in financial records in third party hands,[20] "because the constitutionally protected right, freedom to associate freely and anonymously, will be chilled equally whether the associational information is compelled from the organization itself or from third parties."[21] This distinction between is directly relevant to metadata surveillance, which involves data collected from third party service providers.

Government acquisition of associational information threatens freedom of association because government awareness of citizens' associational choices can be abused and because expressive association may be "chilled" when membership information is in government hands. While the potential impairment of freedom of association must not be merely speculative,[22] evidence of previous harassment[23] is not required. Declarations "attesting to the impact compelled disclosure would have on participation [in the association] and formulation of strategy"[24] have been found sufficient. Moreover,

[19] See e.g., Local 1814, International Longshoremen's Ass'n v. Waterfront Comm'n, 667 F.2d 267 (2d Cir. 1981); NY Times v. Gonzalez, 459 F.3d 160 (2d Cir. 2006); In re Grand Jury Subpoena, 842 F.2d 1229 (11th Cir. 1988); Paton v. La Prade (D.N.J. 1978); US v. Citizens State Bank (8th Cir. 1980); In re Grand Jury Subpoena (10th Cir. 1983); Rich v. City of Jacksonville (M.D. Fla. 2010); Malibu Media v. Does 1-15 (E.D. Pa. 2012)

[20] U.S. v. Miller

[21] In Re First National Bank, 701 F.2d 115 (10th Cir. 1983) (also collecting cases). See also In re Grand Jury Proceeding, 842 F2d 1229, 1233 (11th Cir. 1988) (rejecting argument that the first amendment affords no "extra margin of privacy" by imposing substantive or procedural restrictions on good faith criminal investigations beyond the limits imposed by the fourth and fifth amendments."); 593 F.2d at 1071 n. 4, (Robinson, J., concurring) ("[T]he analysis appropriate for First Amendment issues concentrates on the burden inflicted on protected activities, and the result may not always coincide with that attained by application of Fourth Amendment doctrine."); New York Times v. Gonzalez (2d Cir. 2006) ("whatever rights a newspaper or reporter has to refuse disclosure in response to a subpoena extends to the newspaper's or reporter's telephone records in the possession of a third party provider"). Cf. Reporters Comm. for Freedom of the Press v. AT&T, 593 F.2d 1030, 1054 (D.C. Cir. 1978) ("In my view, the guarantees of the Fourth and fifth Amendments achieve their purpose and provide every individual with sufficient protection against good faith investigative action for the full enjoyment of his First Amendment rights of expression") (portion of majority opinion joined only by Wilkey, J.)

[22] Buckley v. Valeo, U.S. 1 (1976)

[23] See, e.g., Lassa v. Rongstad, 718 N.W.2d 673, 691 (Wis. 2006) (collecting cases).

[24] Perry v. Schwarzenegger, 591 F.3d 1147, (9th Cir. 2010). See also Sneddigar v. Hoddersen, 786 P.2d 781, 785 (Wash. 1990).

courts sometimes find a freedom of association burden "inevitable" as a matter of "common sense"[25] or hold "private association affiliations and activities" "presumptively immune from inquisition."[26]

**B. Freedom of Association, Strict Scrutiny and Specificity**

Strict scrutiny traditionally has been viewed as a kind of trump card.[27] As courts found it necessary or desirable to take conflicting values into account, they developed alternative, "intermediate" levels of scrutiny.[28] Thus, for example, in the free speech context, content-neutral "time, place, or manner regulations" [29] and content regulations with incidental effects on speech are subject to intermediate scrutiny."[30] The idea that strict scrutiny always deals a fatal blow has been undercut in recent years, in part by empirical study demonstrating that regulations do, in fact, survive it.[31]

Freedom of association doctrine generally has not followed the path of accommodating competing concerns by introducing intermediate levels of scrutiny.[32] Instead, cases involving compelled disclosure of associational information have accommodated competing concerns within a strict or

[25] Local 1814, Int'l Longershoremen's Ass'n v. Waterfront Comm'n, 667 F.2d 267, 272 (2d Cir. 1981); In re Grand Jury Subpoena, 701 F.2d 115, 118 (10th Cir. 1983); Tree of Life Christian Schools v. City of Upper Arlington (S.D. Ohio 2012)
[26] Britt v. Superior Ct., 574 P.2d 766, 773 (Cal. 1978). See also Local 1814 at 271-72, quoting Pollard v. Roberts, 283 F. Supp. 248, 258 (E.D. Ark. 1968), aff'd per curiam, 393 U.S. 14 (1968) ("it would be 'naïve' not to recognize that disclosure would impermissibly discourage the exercise of constitutional rights"); Australian/Eastern USA Shipping v. USA (DDC 1982);
[27] See, e.g., Adam Winkler, Fatal in Theory and Strict in Fact: An Empirical Analysis of Strict Scrutiny in the Federal Courts, 59 Vand. L. Rev. 793 (2006) (describing this "myth" and quoting Laurence Tribe as saying "there are very few cases which strictly scrutinize and yet uphold instances of impaired fundamental rights").
[28] See, e.g., Richard H. Fallon, Jr., Strict Judicial Scrutiny, 54 UCLA L. Rev. 1267 (discussing the impact of various intermediate scrutiny tests on the role of strict scrutiny)
[29] Ward v. Rock Against Racism, 491 U.S. 781 (1989).
[30] U.S. v. O'Brien, 391 U.S. 367 (1968).
[31] See Winkler. The study showed that religious liberty regulations were most likely to survive strict scrutiny. Tantalizingly, Winkler's results show freedom of association cases as next most likely to survive strict scrutiny, with free speech cases least likely to survive it. Unfortunately, the differences are not statistically significant so one can only speculate that they would hold up with a larger sample size.
[32] Scrutiny of certain election regulations is the exception to this rule. Clingman v. Beaver, 544 U.S. 581 (2005) ("When a state electoral provision places no heavy burden on associational rights, a State's important regulatory interests will usually be enough to justify reasonable, nondiscriminatory restrictions.") Clingman's lower standard does not apply to mandated disclosure of association membership or affiliation even in the election context. See, e.g., Doe v. Reed (applying "exacting scrutiny" to disclosure of signers of referendum petition); Buckley v. Valeo (applying strict scrutiny to uphold mandated disclosure of political contributions).

"exacting" scrutiny rubric.[33] In some cases, such as *NAACP v. Alabama*, courts find no compelling state interest in acquiring membership information, often because the government's request is driven primarily by animus toward the association in question.[34] In many, if not most, cases, however, the compelling interest requirement is met and the analysis focuses on whether there is a sufficiently tight nexus between the compelling interest and the particular information requested.

In *Shelton v. Tucker*, the Supreme Court focused on the overbreadth of a statute requiring that teachers annually disclose to the state all organizations to which they had belonged within the preceding five years. Though *Shelton* had its roots in hostility toward the NAACP,[35] the Court mentioned that context only in a footnote, specifically distinguishing cases, such as *NAACP v. Alabama*, in which the state's purported interest was spurious. *Shelton*'s analysis began by acknowledging a tension between two propositions: that "there can be no question of the relevance of a State's inquiry into the fitness and competence of its teachers," and that "it is not disputed that to compel a teacher to disclose his every associational tie is to impair that teacher's right of free association … which, like free speech, lies at the foundation of a free society." The impairment resulted from the breadth of the required disclosure:

---

[33] For the most part, courts do not distinguish between "strict scrutiny" and "exacting scrutiny" when dealing with government acquisition of associational information. See, e.g., Buckley v. Valeo, 45, 64, 75 ("[T]he constitutionality of [expenditure limitation] turns on whether the governmental interests advanced in its support satisfy the exacting scrutiny applicable to limitations on core First Amendment rights of political expression." "We long have recognized that significant encroachments on First Amendment rights of the sort that compelled disclosure imposes cannot be justified by a mere showing of some legitimate governmental interest. Since NAACP v. Alabama we have required that the subordinating interests of the State must survive exacting scrutiny." "In considering this provision we must apply the same strict standard of scrutiny, for the right of associational privacy developed in NAACP vs. Alabama derives from the rights of the organization's members to advocate their personal points of view in the most effective way.") In Doe v. Reed, 130 S. Ct. 2811 (2010), however, which uphold disclosure of the names of referendum petition signers, distinguished strict scrutiny from a somewhat more permissive standard of "exacting scrutiny" taken from "precedents concerning disclosure requirements in the electoral context." But see id. at 2839 (Thomas, J., dissenting) ("I read our precedents to require application of strict scrutiny to laws that compel disclosure of protected First Amendment association."). The electoral context" to which the distinction applies is narrowly defined. See id. at 2822 (Breyer, J., concurring) ("where a law significantly implicates competing constitutionally protected interests in complex ways, the Court balances interests"); id. at 2828 (Sotomayor, J., concurring) ("Public disclosure of the identity of petition signers, which is the rule in the overwhelming majority of States that use initiatives and referenda, advances States' vital interests in preserving the integrity of the electoral process, preventing corruption, and sustaining the active, alert responsibility of the individual citizen in a democracy for the wise conduct of government.") Cf. McIntyre v. Ohio (striking down regulation forbidding anonymous campaign pamphlets under strict scrutiny).

[34] See, e.g., Bates v. City of Little Rock; Baird v. State Bar of Arizona;

[35] The lower court also had invalidated a state statute making state employment of NAACP members unlawful.

> The scope of the inquiry required by Act 10 is completely unlimited. The statute requires a teacher to reveal the church to which he belongs, or to which he has given financial support. It requires him to disclose his political party, and every political organization to which he may have contributed over a five-year period. It requires him to list, without number, every conceivable kind of associational tie-social, professional, political, avocational, or religious.

The harm was exacerbated by each school board's unfettered discretion "to deal with the information as it wishes," with the result that "the pressure upon a teacher to avoid any ties which might displease those who control his professional life would be constant and heavy." The Court did not consider whether the plaintiffs' NAACP affiliations, in particular, would expose them to harassment or ill-treatment. The breadth of the mandated disclosure left all teachers uncertain as to whether their associations might be displeasing to someone in a position of power. The statute's "unlimited and indiscriminate sweep" also undermined its fit to the state's purported interest, since many of the relationships disclosed "could have no possible bearing upon the teacher's occupational competence or fitness."

Other cases similarly turn on the fact that demands for membership information are "sweeping and indiscriminate." In *In re Stolar*, for example, the Court struck down a state bar committee's demand that applicants list their association memberships,[36] despite the legitimate state interest in investigating character and competence to practice law. The Court emphasized the burden imposed by the breadth of the inquiry: "[T]he listing of an organization considered by committee members to be controversial or "subversive" is likely to cause delay and extensive interrogation or simply denial of admission to the Bar. … Law students who know they must survive this screening process before practicing their profession are encouraged to protect their future by shunning unpopular or controversial organizations."

[36] 401 U.S. 23 (1971) See also *Baird v. State Bar Ass'n of Arizona*, 401 U.S. 1, 6 (1971) ("Broad and sweeping state inquiries into [associations] discourage citizens from exercising rights protected by the Constitution.") See also Clark v. Library of Congress, 750 F.2d 89, 104 (D.C. Cir. 1984) ("broad and sweeping inquiry into [plaintiff's] political beliefs and associations" must be "justified by a showing that the investigation was necessary to serve a vital governmental interest" and used the "means least restrictive" of first amendment rights"); Britt v. Superior Ct., 574 P.2d 766 (Cal. 1978) ("In view of the sweeping scope of the discovery order at issue, we think it clear that such order is likely to pose a substantial restraint upon the exercise of First Amendment rights");

In *Buckley v. Valeo*,[37] by contrast, the Supreme Court upheld a provision broadly mandating disclosure of political contributions. The Court declined to adopt an intermediate scrutiny, however, opining that "the strict test established by *NAACP v. Alabama* is necessary because compelled disclosure has the potential for substantially infringing the exercise of First Amendment rights." The Court upheld the mandate based on government interests tied closely to the potential impact of campaign contributions on democracy: 1) providing the electorate with information to aid them in evaluating candidates; 2) deterring corruption and avoiding the appearance of corruption; and 3) gathering data needed to detect violations of the statute's contribution limitations. Though disclosure placed "not insignificant burdens on individual rights," it appeared to be the "least restrictive means of curbing the evils of campaign ignorance and corruption that Congress found to exist." Despite noting that freedom of association burdens were heightened and government interests lessened for contributions to minor parties, the Court declined to create a blanket exemption. A few years later, however, the Court voided a similar mandate as applied to the Socialist Workers Party in light of "substantial evidence of past and present hostility from private persons and Government officials" toward the SWP, coupled with the diminished government interests in disclosure in the case of a minor party.[38]

A disclosure mandate need not sweep as broadly as the *Shelton* provision to be unconstitutionally overbroad in relation to the government's need for associational information. In a civil suit brought against airport authorities by a group of local residents, for example, the California Supreme Court quashed a discovery request for all documents reflecting the plaintiffs' communications with several organizations engaged in advocacy relating to noise and other issues concerning the airport. The court opined that "[t]he very breadth of the required disclosure establishes that the trial court in this case did not apply traditional First Amendment analysis in passing on the validity of defendant's inquiries into

[37] U.S. 1 (1976)
[38] Brown v. Socialist Workers '74 Campaign Committee, 459 U.S. 87 (1982).

the private associational realm, and in particular did not heed the constitutional mandate that precision of disclosure is required so that the exercise of our most precious freedoms will not be unduly curtailed."[39]

Freedom of association's specificity requirement is also evident in a number of cases in which courts tailor disclosure mandates, rather allowing or denying them wholesale.[40] For example, in a case alleging that longshoremen had been coerced into authorizing payroll deductions for contributions to a union-related political advocacy organization, the court limited a subpoena for members' names to a random 10% sample of those who had signed up for the deduction relatively late, on the rationale that they were most likely to have been coerced. The limitations were fashioned to ensure that disclosure would "impact a group properly limited in number in light of the governmental objective to be achieved."[41] Courts also have taken steps such as in camera review of evidence and requiring that names of donors be replaced by numbers to protect their identities.[42]

Intrusion into the freedom of association of a legitimate, but unpopular or dissident, group cannot be justified by the mere fact that the investigation aims to determine whether the group has been infiltrated by actors devoted to violent or illegal ends. In *Gibson v. Florida Legislative Investigation Committee*,[43] a legislative committee sought a list of NAACP members, purportedly to determine whether the NAACP had been infiltrated by members of the Communist Party. Communist Party membership was "itself a permissible subject of regulation and legislative scrutiny" due to the

---

[39] Britt at 861.

[40] See, e.g., Matter of Full Gospel Tabernacle; In re Grand Jury Subpoena for Locals 17, 135, 257, and 608 (NY); Doyle v. NYS Div. Housing (SDNY); Nat'l Org. for Marriage v. Maine Comm'n Governmental Ethics (Me.); In re Grand Jury Proceeding (11th Cir.); St. German of Alaska v. USA (2d Cir.) But see Friends Social Club v. Sec'y of Labor (ED Mich); Tree of Life Christian Schools v. City of Upper Arlington (S.D. Ohio) (Although the donor's identity is relevant within the broad confines of *Rule 26*, the Court is not convinced that the donor's identity is "highly relevant" to this case" as required for First Amendment purposes)

[41] Local 1814, Int'l Longshoremen's Ass'n v. Waterfront Comm'n (2d Cir. 1981). See also, e.g. U.S. v. Citizens State Bank (8th Cir. 1980) (suggesting a graduated series of disclosures of associational information); Socialist Workers Party v. Att'y Gen. (2d Cir.) (overturning preliminary injunction on undercover investigation, but retaining injunction against sending members' names to Civil Service Commission); FEC v. Larouche Campaign (2d Cir.) (FEC justified in obtaining names of contributors, but not in obtaining the names of those who solicited contributions)

[42] In re Deliverance Christian Church (ND Ohio)

[43] 372 U.S. 539 (1963).

"particular nature" of that party, but "[v]alidation of the broad subject matter under investigation does not necessarily carry with it automatic and wholesale validation of all individual questions, subpoenas, and documentary demands." The demand for the membership list of a "concededly legitimate and nonsubversive organization" ran afoul of the nexus requirement. Even when upholding a statute requiring "Communist-action organizations" to disclose membership information, the Court emphasized that the designation was made via administrative hearing and subject to judicial review[44] and that "communist-action organization" was defined narrowly as a group "directed, dominated, or controlled" by and operating "primarily to advance the objectives" of a foreign Communist government.

These and other cases demonstrate that specificity requirements stemming from the First Amendment's freedom of association guarantees cabin the amount of information government may demand, especially when government interests are vague and use of the information is left to the discretion of government officials, and permit government acquisition only when there is a close nexus between a specific compelling government interest and the particular information to be acquired, as well as a lack of substantially less intrusive means to accomplish the government's purpose. Like the particularity requirements associated with the Fourth Amendment, these specificity requirements should play an important and direct role in regulating government surveillance of expressive associations.

### C. Freedom of Association Specificity and "Good Faith Investigation"

The argument that the freedom of association imposes specificity requirements on surveillance of expressive associations flies in the face of the government's contention, in justifying the NSA's telephony metadata surveillance, that "otherwise lawful investigative activities conducted in good faith – that is, not for the purpose of deterring or penalizing activity protected by the First Amendment – do not violate the First Amendment."[45] That bald assertion stems from an improper reading of the "good faith"

[44] Communist Party v. Subversive Activities Control Bd. (1961)
[45] White Paper.

standard. As some courts have recognized, the good faith requirement must be interpreted more rigorously to comply with freedom of association's strictures. The good faith investigation standard arises out of two lines of case -- one dealing with arguments for reporter's privileges and another dealing with undercover investigations. The government relies heavily on *Reporters Committee for Freedom of the Press v. AT&T*, which dealt with grand jury subpoenas for journalists' phone records. There, the D.C. Circuit interpreted *Branzburg v. Hayes*, in which the Supreme Court had upheld subpoenas compelling journalists to testify about articles they had published based on confidential sources.[46]

As the Court explained in *Branzburg*:

> The sole issue before us is the obligation of reporters to respond to grand jury subpoenas as other citizens do and to answer questions relevant to an investigation into the commission of crime. … The claim is [] that reporters are exempt from these obligations because if forced to respond to subpoenas and identify their sources or disclose other confidences, their informants will refuse or be reluctant to furnish newsworthy information in the future. This asserted burden on news gathering is said to make compelled testimony from newsmen constitutionally suspect and to require a privileged position for them.

The Court refused to confer a special privilege against grand jury subpoenas on journalists, pointing out that grand juries remain "subject to judicial control and subpoenas to motions to quash" if appropriate in particular cases. A concurrence by Justice Powell further emphasized that "case-by-case basis" motions to quash could "strik[e] the proper balance between freedom of the press and the obligation of all citizens to give relevant testimony with respect to criminal conduct." In any event, the Court opined, the subpoenas at issue in *Branzburg* met the standards set out in its membership list disclosure cases. The Court also observed that "grand jury investigation, if instituted or conducted other than in good faith, would pose wholly different issues for resolution under the First Amendment."

In *Reporters Committee*,[47] a group of journalists challenged the use of grand jury and administrative subpoenas to acquire their calling records from their carriers, seeking notice and an opportunity for

[46] 408 US 665 (1972).
[47] 593 F.2d 1030 (1978)

judicial review before such records were disclosed.[48] Anticipating the Supreme Court's ruling in *Smith v. Maryland*,[49] the D.C. Circuit held that the Fourth Amendment was inapplicable to third party phone records.[50] The majority interpreted *Branzburg* to hold that "there is no case-by-case consideration given to a claim of privilege," and thus concluded that journalists "have no right to resist good faith subpoenas duces tecum directed at a third-party's business records." As a dissent was quick to point out, however, *Branzburg* "turned explicitly on the fact that the prior judicial scrutiny on a case-by-case basis which was afforded [by a motion to quash] was sufficient to protect the First Amendment rights at stake."

The *Reporters Committee* reading of *Branzburg* has been rejected by many other courts.[51] The Second Circuit, for example, explicitly rejected it, holding that subpoenas for reporters' phone records are subject to First Amendment balancing. Consistent with freedom of association's specificity requirement, the Second Circuit suggested that a request for "disclosure of all phone records over a period of time" might be overbroad as yielding "information that bears only a remote and tenuous relationship to the investigation," and suggested that such overbreadth might be cured by redaction of unrelated records.[52] Most importantly, *Branzburg* and *Reporters Committee* did not involve government demands for association membership information, but focused on whether journalists should be granted blanket privileges.[53] *Reporters Committee* is thus a weak reed on which to stand an argument that legitimate intentions inoculate government investigations from First Amendment scrutiny.

---

[48] Reporters Comm. For Freedom of the Press v. AT&T, 593 F.2d 1030 (D.C. Cir. 1978)
[49] [cite]
[50] Reporters Committee at 1043. The majority opinion also opined that freedom of association cases, such as NAACP v. Alabama "do not apply to the good faith collection of information about third parties," a position which, as discussed above, has been largely rejected by later courts.
[51] See, e.g., NY Times v. Gonzales; Local 1814, Int'l Longshoremen's Ass'n; In re Grand Jury Subpoena (Miller) (2d Cir.) (concurrence); In re Grand Jury Proceeding (11th Cir.), In re Grand Jury Subpoena to First National Bank (10th Cir.); Paton v. La Prade (DNJ); US v. Markiewicz. See also United Transp. Union v. Springfield (declining to follow in civil context); Philip Morris v. ABC (same). See also Parson v. Watson (D.Del.) (discussing various readings of Branzburg).
[52] NY Times v. Gonzales.
[53] *Zurcher v. Stanford Daily*, another foundation for the argument that First and Fourth Amendment protections are nearly coterminous, concerned a similar issue: whether news organizations should be subject to search warrants for evidence of third party criminal activity. It did not involve a government attempt to acquire associational information.

The other thread of cases involving the good faith investigation standard deals with undercover investigation of political and religious organizations. Because undercover agents and informers often seek information about the identities of association members, these cases are more relevant to the issue considered here. Courts generally agree that "the use of secret informers or undercover agents is a legitimate and proper practice of law enforcement and justified in the public interest."[54] "The government is not limited to investigating crimes already fully consummated. If an organization advocates terrorist acts, … the government surely could investigate it … even if the advocacy were protected by the First Amendment because it was not directed to 'producing imminent lawless action' and was not likely to do so."[55] The First Amendment "protects individuals against excesses and abuses in such activities,"[56] however, and while activities aimed directly at disrupting or countering an association's expression clearly are prohibited,[57] good intent "cannot be the sole test of legitimacy."[58]

When there is a "potential for interference with protected associational and expressive interests" in an undercover investigation, courts sometimes employ standard freedom of association scrutiny. For example, the D.C. Circuit held that an FBI "full field investigation" into a Library of Congress employee based on his involvement with a controversial but non-violent political organization violated his freedom of association rights because the government did not show that the investigation was "necessary to serve a vital governmental interest" or "that the full field investigation was the available means least restrictive of Clark's first amendment rights."[59] In *Paton v. La Prade*, the court struck down a statute authorizing the use of "mail covers" (regular recording of address information on an entity's mail) "to protect the national security." Though address information is exempt from Fourth Amendment

[54] Handschu v. Special Servs. (SDNY 1972)
[55] ACLU v. Barr (D.C. Cir. 1991)
[56] Handschu
[57] Hobson v. Wilson (D.C. Cir. 1984) ("it is never permissible to impede or deter lawful civil rights/political organization, expression or protest with no other direct purpose and no other immediate objective than to counter the influence of the target associations")
[58] Clark v. Library of Congress (D.C. Dir. 1984).
[59] *Clark v. Library of Congress* 750 F.2d 89, 98 (D.C. Cir. 1984)

protection because it is in "plain view," the provision failed freedom of association scrutiny because government's general interest in "[n]ational security as a basis for the mail cover is unconstitutionally vague and overbroad, leaving too much discretion to government officials."[60] In *Pleasant v. Lovell*,[61] the court denied qualified immunity as to First and Fourth Amendment claims based on an IRS investigation of a tax protest organization in which an informant in charge of removing and burning the organization's trash had surreptitiously seized non-trash documents, including a mailing list. The court noted that while "some interference [with freedom of association] may be permissible when the government can demonstrate a compelling interest, such as good-faith criminal investigation that is narrowly tailored to detect information concerning tax evasion," the seizures of non-trash documents "may constitute government interference with the freedom to associate …."

Other cases approach freedom of association challenges to undercover investigations differently. They note that Fourth Amendment expectations of privacy often are vitiated in these investigations either by the fact that meetings are open to the public or by the "invited informer" doctrine, under which there is no reasonable expectation of privacy with regard to undercover informants because individuals "assume the risk" that those in whom they have placed confidence may betray them.[62] These courts assess freedom of association claims using "two general principles:" that the investigation "be conducted in good faith" and that "undercover informers adhere scrupulously to the scope of a defendant's invitation to participate in the organization."[63] The Ninth Circuit recently has explained that,

---

[60] See also Tabbaa v. Chertoff , 509 F.3d 89, (2d Cir. 2007)( "Our conclusion that the searches constituted a significant or substantial burden on plaintiffs' First Amendment associational rights is unaltered by our holding that the searches were routine under the Fourth Amendment. As is clear from the above discussion, distinguishing between incidental and substantial burdens under the First Amendment requires a different analysis, applying different legal standards, than distinguishing what is and is not routine in the Fourth Amendment border context."

[61] 876 F.2d 787, 804 (10th Cir. 1989);

[62] Lopez; White

[63] Alvarez; Mayer; Pleasant; Jabara; Presbyterian Church; See also Voss v. Bergsgaard, 774 F.2d 402, 405 (10th Cir. 1985) (Search warrant authorizing seizure of documents, including "indicia of membership in or association with the NCBA" from organization engaging both in anti-tax advocacy and in potentially fraudulent transactions designed to avoid tax

despite phrasing in earlier opinions suggesting that "good faith" merely means good intentions,[64] good faith demands that "an investigation threatening First Amendment rights … be justified by a legitimate law enforcement purpose that outweighs any harm to First Amendment interests,"[65] a test similar to standard freedom of association scrutiny.

Two district court opinions are illuminating in this regard. In *Jabara v. Kelley*,[66] the court opined that "the first amendment and the fourth amendment provide coextensive zones of privacy in the context of a good faith criminal [or national security] investigation" because "[t]o tailor investigations so as to avoid implicating a subject's first amendment activities would be impossible." Nonetheless, "'good faith national security investigation' suggests more than a subjective perception of a threat to the national security, it suggests an investigation which is in response to a demonstrable threat to the nation or its citizens and which is calculated to deal with or provide information regarding that threat." *Jabara* challenged a multi-year national security investigation of an attorney who was an active participant in various Arab organizations. The court denied the government's motion for summary judgment on the good faith issue, questioning the fit between the "generalized and legitimate" national security concerns that "provided the impetus for the investigation" and the "length of the investigation, its seeming preoccupation with Jabara's political views" and other factors tending to indicate that the investigation "was not wholly prompted by legitimate or good faith national security concerns."

In *Presbyterian Church v. United States*,[67] the court considered a challenge to an immigration service investigation of churches participating in the "sanctuary movement" for Central American refugees. Employing standard First Amendment scrutiny, the court held that the government interest in

---

obligations not only lacked sufficient particularity to satisfy the fourth amendment, but was "particularly infirm given that speech and associational rights of NCBA members were necessarily implicated.")

[64] U.S. v. Aguilar

[65] U.S. v. Mayer

[66] 476 F. Supp. 561 (E.D. Mich. 1979);

[67] 752 F. Supp. 1505 (D. Ariz. 1990), on remand from Presbyterian Church v. United States, 870 F.2d 518 (9th Cir. 1989) (finding standing for freedom of association claim)

border security was compelling. It then considered the fit between that interest and the investigation's scope and tactics, rejecting the plaintiffs' argument that subpoenas and surveillance outside of church meetings were adequate alternatives. In its analysis, the court interpreted the good faith and scope of the invitation requirements as ways of implementing the First Amendment's least restrictive means test.

The conflicting and somewhat muddled case law in this area reflects judges' attempts to reconcile competing concerns. On the one hand, courts are uneasy about interfering with executive branch discretion in conducting investigations[68] and believe that undercover investigation is a necessary and important investigative tool. On the other hand, they are equally concerned with granting government officials excessive discretion[69] to interfere with freedom of association, especially in light of past abuses. As the Supreme Court has explained in the Fourth Amendment context:

> These Fourth Amendment freedoms cannot properly be guaranteed if domestic security surveillances may be conducted solely within the discretion of the Executive Branch. The Fourth Amendment does not contemplate the executive officers of Government as neutral and disinterested magistrates. Their duty and responsibility are to enforce the laws, to investigate, and to prosecute. But those charged with this investigative and prosecutorial duty should not be the sole judges of when to utilize constitutionally sensitive means in pursuing their tasks. The historical judgment, which the Fourth Amendment accepts, is that unreviewed executive discretion may yield too readily to pressures to obtain incriminating evidence and overlook potential invasions of privacy and protected speech.[70]

While made in a Fourth Amendment case, these remarks are directly applicable to freedom of association in the investigation context. Emphasizing the specificity demanded by freedom of association illuminates commonalities between cases applying freedom of association scrutiny directly and cases taking the good faith and scope of the invitation approach. These approaches are best viewed

[68] See, e.g., Reporters Committee.
[69] See, e.g., Stanford v. Texas; Zurcher v. Stanford Daily; Presbyterian Church v. United States, 752 F. Supp. 1505 (D. Ariz. 1990) ("The government, however, does not have unfettered discretion to conduct investigations and law enforcement activities. The first amendment limits the government's ability and authority to engage in these activities when groups are engaged in protected first amendment activities.")
[70] U.S. v. U.S. Dist. Ct. (Keith case), 407 U.S. 297 (1972)

as alternative means to ensure the tight fit between means and ends demanded by the right to freedom of association. Interpreting "good faith" as merely "good intentions" is inconsistent with that requirement.

## II. Metadata Surveillance, Overbreadth, and Specificity

Because the NSA's telephony metadata program recently has been the subject of Congressional hearings, legal complaints, and public debate, I use it here as a lens through which to consider the implications of freedom of association's specificity requirements for metadata surveillance.[71]

### A. The Telephony Metadata Surveillance Program

Recent leaks have revealed that the NSA collects "all call detail records or 'telephony metadata' created by [major carriers] for communications (i) between the United States and abroad; or (ii) wholly within the United States, including local telephone calls."[72] This data collection is purportedly authorized under § 50 USC 1861 of FISA (commonly known as "Section 215 of the Patriot Act"). FISA was enacted in 1978 as part of a major overhaul of surveillance law in response to widespread abuses during the 1960s and 70s. It established a set of requirements for judicial oversight of foreign intelligence surveillance. For example, to authorize electronic surveillance of communication content, it required a warrant based on "probable cause to believe that the target" was "a foreign power or an agent of a foreign power."[73]

Most relevant for present purposes, FISA contained a number of provisions regulating the collection of metadata. It authorized the FISC to issue "pen register" orders for interception of "dialing, routing, addressing, or signaling information"[74] upon the submission of "information which demonstrates that there is reason to believe that the [communication device at issue] has been or is about

[71] However, the conceptual arguments made here do not depend very heavily on details about the NSA's metadata surveillance program. While the NSA is probably on the cutting edge, there is every reason to believe that metadata surveillance is becoming part and parcel of the law enforcement toolbox. See article about DEA's Hemisphere program.
[72] See, e.g., In Application of the FBI for an Order Requiring the Production of Tangible Things from Verizon Business Network Services, No. BR 13-80 (F.I.S.C. July 19, 2013).
[73] 18 USC 1801, 1802
[74] 18 USC 3127. Definition incorporated by reference into 50 USC 1841.

to be used in communication with- (A) an individual who is engaging or has engaged in international terrorism or clandestine intelligence activities that involve or may involve a violation of the criminal laws of the United States; or (B) a foreign power or agent of a foreign power under circumstances giving reason to believe that the communication concerns or concerned international terrorism or clandestine intelligence activities that involve or may involve a violation of the criminal laws of the United States."[75] It also authorized the use of "national security letters," available without court authorization, to obtain "name, address, length of service, and toll billing records" upon certification that "(1) the information sought is relevant to an authorized foreign counterintelligence investigation; and (2) there are specific and articulable facts giving reason to believe that the person or entity to whom the information sought pertains is a foreign power or an agent of a foreign power."[76] In 1998, Congress added a provision authorizing FISC orders for the production of certain business records, including "records from common carriers, public accommodation facilities, storage facilities, and vehicle rental facilities," if the application contained ""specific and articulable facts giving reason to believe that the person to whom the records pertain is a foreign power or an agent of a foreign power."[77]

Shortly after the September 11th, 2001, terrorist attacks, the USA Patriot Act expanded foreign intelligence surveillance authorities. Pen register availability was extended to "any investigation to obtain foreign intelligence information not concerning a United States person or 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" upon certification that "the information likely to be obtained is relevant to an ongoing

[75] 18 USC 1842 (original version)
[76] 18 USC 2709 (original version)
[77] CRS Amendments to FISA. 50 USC 1862(b)(2)(B)(2001).

investigation to protect against international terrorism or clandestine intelligence activities."[78] National security letter authority for telephone transaction records was extended to require certification only that "the name, address, length of service, and toll billing records sought are relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities, provided that such an investigation of a United States person is not conducted solely on the basis of activities protected by the first amendment to the Constitution of the United States."

Most relevant to the controversy over the NSA's collection of telephony metadata, Section 215 of the Patriot Act expanded the business records provision substantially to permit "an application for an order requiring the production of any tangible things (including books, records, papers, documents, and other items)".[79] The application for a Section 215 order must include:

> (A) a statement of facts showing that there are reasonable grounds to believe that the tangible things sought are relevant to an authorized investigation (other than a threat assessment) conducted [in accordance with Attorney General guidelines] and to obtain foreign intelligence information not concerning a United States person or 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] … .

All of these provisions authorizing the collection of metadata now employ a relevance threshold. The standards for FISA pen registers, Section 215 orders, and national security letters are compared explicitly in the legislative history to the standards for pen registers in the law enforcement context, grand jury subpoenas, and administrative subpoenas, respectively.

At around the same that the Patriot Act was enacted, two metadata surveillance programs began. The NSA began collecting telephone metadata as part of what became known as the "President's

[78] 18 USC 1842. This relevance standard mirrors that in the criminal context, where a court order for interception of call traffic data requires certification certify only "that the information likely to be obtained is *relevant* to an ongoing criminal investigation." 18 U.S.C. § 3122 (2000) (emphasis added).
[79] 18 USC 1861.

Surveillance Program."[80] The PSP was authorized solely by executive order and supported by opinions from the Department of Justice's Office of Legal Counsel. Its goal was to employ "contact chaining" to uncover terrorist networks. As described in an NSA Inspector General Report, "contact chaining is the process of building a network graph that models the communication (e-mail, telephony, etc.) patterns of targeted entities (people, organizations, etc.) and their associates from the communications sent or received by the targets." This process is commonly known as "social network analysis."

The Defense Advanced Research Projects Agency (DARPA) also began a program known as Total Information Awareness, which promised to determine how to use data from "the transaction space" (i.e., metadata) to "pick the [terrorist] signal out of the noise."[81] One of TIA's components was "Link and Group Understanding," in which software was to be developed to "discover linkages among people, places, things, and events related to possible terrorist activity.[82] It was to include "Scalable Social Network Analysis"[83] "to extend techniques of social network analysis to assist with distinguishing potential terrorist cells from legitimate groups of people, based on their patterns of interactions, and to identify when a terrorist group plans to execute an attack." Media reports about TIA raised a firestorm of controversy. In response, Congress eventually defunded it in October 2003.

In 2006, Congress added a "minimization procedures" requirement to Section 215, restricting the dissemination of information about United States persons and clarified that a Section 215 order "may only require the production of a tangible thing if such thing can be obtained with a subpoena duces tecum issued by a court of the United States in aid of a grand jury investigation or with any other order issued by a court of the United States directing the production of records or tangible things." The legislative history explains that "[p]rior and subsequent to enactment of the USA PATRIOT Act, law

[80] NSA Inspector General Report (March 24, 2009).
[81] http://www.fas.org/irp/agency/dod/poindexter.html
[82] http://www.information-retrieval.info/docs/tia-exec-summ_20may2003.pdf at 3.
[83] http://epic.org/privacy/profiling/tia/may03_report.pdf.

enforcement could obtain records from all manner of businesses through grand jury-issued subpoenas. … Section 215 of the USA PATRIOT Act created similar authority, but with more stringent requirements. …" The legislative history also reports that "the [Section 215] provision to date has been used only to obtain driver's license records, public accommodation records, apartment leasing records, credit card records, and subscriber information, such as names and addresses, for telephone numbers captured through court-authorized pen-register devices.[84]

Soon, however, the NSA began to use the Section 215 business records provision for broad-based collection of telephony metadata.[85] In May 2006, the FISC issued a Section 215 order requiring carriers to produce "comprehensive communications routing information, including but not limited to session identifying information (e.g. originating and terminating telephone number, communications device identifier, etc.), trunk identifiers, and time and duration of call," but excluding "the substantive content of any communication … or the name, address, or financial information of a subscriber or customer."[86] The order mandated that NSA access the collected metadata only "when NSA has identified a known telephone number 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 number is associated with [redacted name]," with the caveat that, for a phone number used by a US person, the determination not be based solely on First Amendment protected activities. The order included various requirements for audit and review and commanded that the data be destroyed after five years.

[84] H. Rept. No. 109-174 (2005); S. Rpt. 109-369 (2005). See also, H. Rpt. No. 112-79 (2012) ("The Section 215 business records authority … is similar to the widely-used grand jury subpoena authority in criminal investigations."); S. Rpt. 112-13 ( )("In criminal matters, similar records may be obtained using a grand jury subpoena");
[85] The Office of Legal Counsel's opinions supporting the collection of bulk internet metadata pursuant to the PSP had been rescinded in 2004.
[86] FISC Order, No. BR 06-05.

The FISC issued renewed authorizations for comprehensive collection of telephony metadata regularly until 2009, when the NSA reported that it had inadvertently conducted numerous metadata queries targeting telephone numbers that did not meet the "reasonable articulable suspicion" (RAS) standard. (Indeed, the government admitted in a court filing that "the majority" of the numbers on its authorized list had not been vetted by the standard.) The FISC ordered the NSA to cease accessing the metadata and to thoroughly review its software and procedures. Various other non-compliance instances were uncovered, including unauthorized sharing of query results within the NSA and with other intelligence agencies and analyst use of queries to pursue personal agendas.[87] The FISC eventually reauthorized the metadata collection, though with somewhat stricter provisions. In particular, querying was limited to metadata within three "hops" of a telephone number meeting the RAS standard.

In 2013, the FISC released two opinions considering the legality of comprehensive telephony metadata collection under Section 215.[88] In the first, the court determined that the government had met the relevance standard, interpreting relevance broadly to mean that the records have "some bearing on [] investigations of the identified international terrorist organization," and stated that the "finding of relevance most crucially depended on the conclusion that bulk collection is necessary for NSA to employ tools that are likely to generate useful investigative leads," so that "the entire mass of collected metadata is relevant to investigating international terrorist groups and affiliated persons." The court also held that the program's constitutionality under the Fourth Amendment was "squarely controlled by the U.S. Supreme Court decision in *Smith v. Maryland* …," which held there was no reasonable expectation of privacy in dialed telephone numbers because the numbers were part of the business records of a third

[87] Business Records FISA NSA Review (June 25, 2009); Report of the United States, In re Application of the FBI for an Order Requiring the Production of Tangible Things, No. BR 09-09 (August 17, 2009); Order Regarding Further Compliance Issues (Sept. 25, 2009);

[88] In re Application of the FBI for an Order Requiring the Production of Tangible Things, No. BR 13-109 (Aug. 29, 2013); In re Application of the FBI for an Order Requiring the Production of Tangible Things, No. BR 13-158 (October 11, 2013).

party. In the second opinion, the court held that the Supreme Court's decision in *United States v. Jones* that location tracking using a GPS monitor constituted a search did not change the analysis.

### B. Social Network Analysis as a Tool for Identifying Members of Malevolent Groups

To understand the freedom of association implications of metadata collection, it is helpful to be a bit more specific about the basic types of social network analysis that might be used in a national security or law enforcement context. Social network analysis is based on a set of "nodes" representing individuals or organizations and some means for defining links between them. Telephony metadata, for example, may be used to define links representing connections between phone numbers. The links may be directional (indicating who initiated calls) or weighted (for example, by call frequency) to better reflect social relationships. Government analysts may employ some combination of three basic types of social network analysis: structural analysis of relationships within a known group; targeted link analysis as a means of identifying and categorizing those associated with a target phone number; and pattern-based analysis aimed at matching observed associational patterns to models of malevolent associations.

#### 1. Analysis of Known Social Networks

Sociologists developed social network analysis as a research tool for understanding social relationships using metrics such as "degree" (the number of others to whom a particular individual is linked) and "betweenness" (the extent to which an individual is important in connecting sub-groups). It can help to determine the roles played by various group members and provide insights into group structure and dynamics, perhaps to identify key participants in a criminal or terrorist organization.

#### 2. Targeted Link Analysis to Uncover and Categorize Associations

Targeted link analysis appears to be at the heart of the NSA's justification for comprehensive telephony metadata collection. It begins with a target node, uses "chaining" (following links outward from the target and those connected to the target) to create a map of the network of communications

surrounding the target, and then analyzes the web of relationships in which the target is embedded. In the NSA telephony metadata program, queries begin from a target meeting the RAS standard and go out as many as three hops. The metadata pulled out by a query is transferred to a "corporate store" for further analysis.[89] Based on its analysis, the NSA may "tip" leads to the FBI for further investigation.

The network of metadata pulled out by a single query may be extremely large. Over the five year data storage period, an individual is likely to exchange phone calls with a rather large number of others -- one of my recent phone bills reflected calls to twenty-six numbers during a single month. If an average individual calls 100 distinct numbers over a five year period, who each call 100 others, and so forth, a three-hop query would sweep in around *one million* individuals. If the appropriate one-hop basis is 20, three hops sweep in around 8000 individuals. If it is 500, three hops sweep in around *one hundred million* individuals. The point is not that these numbers are accurate – they are speculative and do not account for important issues such as overlap in numbers dialed by different individuals – but simply that a three-hop query is likely to pull out a very large number of phone numbers indeed.

While centered on a target individual, targeted link analysis aims to expose and analyze associations involving as-yet-unidentified individuals. In the law enforcement or counterterrorism context, the ultimate goal is to create a membership list and social map of a criminal or terrorist organization. Intermediate goals might be to confirm that the target is affiliated with a known malevolent group, to map out the various associational groups to which the target belongs, or to discover unknown members of a malevolent group to which the target is known to belong. A target individual is likely to belong to multiple and overlapping social groups. If it is to be of any practical use, the analysis must somehow disentangle malevolent groups from legitimate associations. There are two basic strategies for doing that: i) analyzing the structure of the network and ii) supplementing the network

[89] In re Application of the FBE for an Order Requiring the Production of Tangible Things, No. BR 13-80, Primary Order (April 25, 2013) at 11. ("The corporate store may then be searched by appropriately and adequately trained personnel for valid foreign intelligence purposes, without the requirement that those searches use only RAS-approved selection terms.")

graph with information from other sources. Indeed, an analyst generally must do both to have any chance of distinguishing malevolent associations from a background of many legitimate associations.

One specific approach might be to supplement the network data with a pre-existing list of members (or suspected members) of a malevolent group and use network analysis to analyze whether the target is densely connected to that group. Previously unidentified individuals who are sufficiently densely connected to the individuals on the list might also be flagged as possible members. Alternatively, one might employ data mining techniques to assign individuals in the target's network to "clusters" or "communities,"[90] by using some metric (such as calling frequency or number of shared contacts) to compare intensities of connections within the cluster to intensities of connections to outsiders. Algorithms for uncovering community structure in network graphs are a subject of ongoing research. The task is particularly difficult for social networks, which are complex, dense, and may include overlapping communities.[91] Many clustering algorithms do not allow for overlaps, assigning each individual to only one community. If such an algorithm is used to cluster metadata for the communications of overlapping communities, the clusters defined by the algorithm unavoidably will mix members of those communities. If, on the other hand, one uses an algorithm that can recognize overlapping clusters, each individual is likely to be assigned to several clusters and additional investigation will be necessary to determine which real world group corresponds to each cluster.

### 3. Pattern-Based Social Network Analysis

Pattern-based analysis[92] begins with (or develops) a model "terrorist" or "criminal" network pattern and searches the network of metadata for similar patterns, under the assumption that similar network patterns are likely to indicate terrorist or criminal activity. Pattern matching can be reasonable

[90] *See*, *e.g.*, Michelle Girvan and M. E. J. Newman, *Community Structure in Social and Biological Networks*, 99 Proc. Natl. Acad. Sci. USA 7821 (2002) for one discussion of a clustering algorithm and its accuracy and computational expense.
[91] *See* WATTS; BARABASI.
[92] Nat'l Academies of Sciences

accurate as long as: 1) patterns for malevolent groups are sufficiently different from normal patterns and 2) neither the malevolent patterns nor the normal patterns change significantly over time. These requirements may not be met for terrorist or criminal networks. Well-characterized examples thankfully are rare, undermining the statistical certainty of historically-derived model patterns. There may or may not even be "typical" metadata patterns for malevolent groups. If not, modeling is not just difficult, but impossible. Even if network patterns typical of malevolent groups exist, there is no particular reason to expect those patterns to be distinguishable from those of legitimate groups.

### C. Social Network Analysis and Specificity

The above sketch of social network analysis suggests several problems with the specificity with which metadata surveillance can advance its core goal of obtaining membership lists and structural information about malevolent groups. Most of these problems are unlikely to be avoided by technical improvements in analysis methods or algorithms.

#### 1. Social Network Analysis of Metadata is Likely to Make Mistakes

##### a. Social Network Analysis Results are only as Good as the Mapping between Metadata and Social Relationships

Network analysis begins by making a map of connections between nodes based on some kind of data and attributing meaning to those connections and nodes. Conclusions drawn from the analysis are trustworthy only if the map itself and the meanings ascribed to the connections and nodes are sufficiently accurate. For example, the map of social relationships produced by telephony metadata consists of nodes representing telephone numbers and links representing telephone calls, perhaps weighted to indicate call frequency. The meaning ascribed to the links is "social relationship," while call frequency may be interpreted as importance, closeness or intensity of relationship.

Many things can go wrong with such a map. First, the phone numbers may be used by more than one individual or an individual may have more than one number. Second, individuals may have

important social relationships with people they never contact by phone, while they may speak frequently by phone to people with whom they have no significant social relationship, such as those taking orders at a favorite pizza parlor. Indeed, these maps may be particularly inaccurate for malevolent groups, which actively seek to minimize the density of traceable connections between members.[93]

**b. Social Network Analysis Cannot Uncover Distinctions that are not Reflected in the Data**

Data mining often seems surrounded by an aura of magic, as it mysteriously uses purchases at Target to predict pregnancy or purchases of beer to predict purchases of diapers. Without downplaying the real potential of data mining, it is critically important to remember that data mining is simply statistical analysis of patterns in data. It may be better than unaided human perception at recognizing patterns in the data, but it can see only patterns that are in the data to see. And it is predictive only to the extent that future patterns are likely to be the same as historical patterns.

The accuracy of social network analysis in discriminating between malevolent and legitimate associations will depend not only on whether the algorithm can recognize overlapping communities, but more fundamentally on the ways in which membership in the malevolent group overlaps with membership in legitimate groups. For example, most members in a malevolent group might also belong to larger religious, political, or social organizations. Social network analysis will not be able to distinguish between overlapping groups unless the underlying metadata reflects significant differences in the relationships between individuals in different groups. If members of a religious or political organization call one another with about the same distribution of frequencies, durations and so forth as do the members of a malevolent sub-group, telephone metadata analysis cannot disentangle the groups.

**c. Community Clustering Algorithms are Fallible.**

[93] Valdis E. Krebs, Uncloaking Terrorist Networks (mapping the network of relations between the September 11th hijackers and discussing the difficulty in identifying terrorist networks before the fact); Greenblatt et al, *supra* note 10 at 344 ("Covert organizations generally do not have many paths of communications flow between individuals. Redundant paths lead to increased risk of exposure or capture.")

Even if the underlying data reflects social relationships reasonably accurately and the analysis employs a top-notch clustering algorithm, there are likely to be some mistaken membership assignments. Moreover, the limitations of a particular set of metadata may be essentially random, for example if individuals simply vary in how often they call those with whom they have similarly strong relationships, or they may be systematic, for example if calling patterns vary systematically by gender, age, ethnicity, income level or some other factor and the data does not reflect those variables.

### 2. Social Network Analysis of Large Metadata Sets Will Produce Membership Lists of Numerous Legitimate Associations

The output of a network clustering analysis is a complete set of community membership lists. To determine which, if any of these relates to a malevolent community, the government will have to investigate each of these communities. For example, suppose that the target of a link analysis is a member of a terrorist organization, a political organization, a religious organization, a business community, and a poker club. Because the memberships of these groups overlap one another, the social network analysis may distinguish only three communities. To determine which (if any) of these communities are likely to be malevolent, the analyst will have to conduct further investigation. That will mean identifying the members of these groups and working backwards to determine the character of the associations. If the three communities correspond to the political, religious, and business groups, the government will end up with membership lists (and additional structural information) for those groups.

In the (unlikely) best case scenario where a social network analysis produces accurate lists of the members of all five communities, the analyst will still have to investigate each community further to determine which (if any) is a malevolent group) and will be in possession of membership lists (and additional structural information) for the legitimate associations. Moreover, each of these legitimate groups now will be connected in intelligence records with a target of an investigation.

Even if some cluster can be identified as a likely malevolent group, law enforcement and counterterrorism officials are unlikely to be content simply to throw out information about legitimate communities identified by the analysis. Such information may well be useful to the investigation of the suspected malevolent group. For example, legitimate groups might usefully be infiltrated to gain access to a target individual or watched as potential "gateways" to participation in the malevolent organization.

### 3. Pattern-Based Social Network Analysis is Likely to Produce Many False Positives

Pattern-based analysis is unlikely to be effective in the national security context or in many law enforcement contexts because metadata patterns associated with malevolent groups are unlikely to be distinguishable from legitimate organizations.[94] To the extent that patterns typical of malevolent organizations reflect their most obvious difference from many legitimate associations -- their covert nature -- they may resemble the patterns of sensitive or disfavored legitimate associations. Moreover, while officials certainly are sensitive to the potential costs of failing to identify malevolent networks, they may be largely insensitive to the costs of intrusions into legitimate associations and false suggestions of association with criminal or terrorist organizations. The costs of false positives may be concentrated on socially disfavored groups, leaving the majority of citizens unaffected. Other costs, such as the chilling of expressive association and generalized avoidance of experimentation with controversial ideas, though potentially great, are sufficiently amorphous that they may not provoke significant complaint. Secrecy and opacity also make it difficult or impossible for citizens to assess the effectiveness of metadata surveillance and to weigh its benefits and costs, further blunting the potential that government officials will internalize the costs of excessive associational surveillance.

## C. Impact on Legitimate Associations

To summarize, social network analysis of the entire metadata network or of a large sub-network produced by chaining is likely to produce approximate membership lists for many more legitimate than

[94] *Id.*; see also Slobogin, *Government Data Mining*; SOLOVE.

malevolent associations. Legitimate associations that share political, religious, or ethnic affiliations with targets of a targeted-link analysis or with associations used as models for pattern analysis are most likely to have their membership lists revealed to the government by such analysis. Moreover, the analysis is likely to have difficulty distinguishing malevolent associations from the background "noise" of legitimate associations (and may not be capable of doing so), prompting further investigation of legitimate associations. Indeed, having obtained membership lists of all legitimate organization that are somehow related to a suspected target, government officials are likely to want to use that information in their investigations, whether or not they have any suspicions about those associations or their members. The situation is closely reminiscent of the burdens imposed on the NAACP when it became a focus of Florida's investigation of subversive activity by the Community Party because state officials suspected that it had been infiltrated. As the Supreme Court explained:

> Compelling such an organization, engaged in the exercise of First and Fourteenth Amendment rights, to disclose its membership presents [] a question wholly different from compelling the Communist Party to disclose its own membership. Moreover, even to say [] that it is permissible to inquire into the subject of Communist infiltration of educational or other organizations *does not mean that it is permissible to demand or require from such other groups disclosure of their membership by inquiry into their records* …. The prior holdings that governmental interest in controlling subversion and the particular character of the Communist Party and its objectives outweigh the right of individual Communists to conceal party membership or affiliations by no means require the wholly different conclusion that other groups -- concededly legitimate -- automatically forfeit their rights to privacy of association simply because the general subject matter of the legislative inquiry is Communist subversion or infiltration. (Emphasis added.)[95]

[95] Gibson v. Florida Legislative Investigation Comm.

## IV. Metadata Surveillance and Freedom of Association Specificity

As discussed in Part I, a government demand for associational information must have a close fit to a specific compelling government interest, government discretion with respect to the use of the information must be adequately cabined and there must be no way to make comparable progress toward the government's compelling ends that is significantly less intrusive on freedom of association. This Part assesses the NSA's comprehensive telephony metadata collection in light of those requirements.

The "broad and sweeping" membership disclosure requirement struck down in *Shelton* pales in comparison to the scope of the NSA's telephony metadata program. If the government were to make a direct inquiry for association membership lists on such a scale based on a general assertion that the lists would "help identify terrorist operatives or networks," there is no chance that the inquiry would pass muster. Though the interest in identifying terrorist operatives or networks is compelling and even if the inquiry were backed up by good intentions, such a mandate would fail on numerous grounds, including: the lack of specificity of the compelling government interest, the unfettered discretion afforded to government officials who received the lists, the lack of a tight fit between membership lists of the vast majority of organizations and the identification of terrorists and the availability of the alternative approach of more focused investigations of particular groups based on specific suspicions that they or their members are involved in terrorist activity. [96]

The NSA would contend, however, that several features of the telephony metadata surveillance program distinguish it from such a plainly unconstitutional inquiry. Specifically, the government argues that "the FISC orders authorizing the program are not targeted at Plaintiffs, based on their associational activities or otherwise; do not compel Plaintiffs or anyone else to disclose the names or addresses of

[96] Stating this example underscores the inadequacy of the government's argument, in briefing in ACLU v. Clapper, that either the lack of a "purpose to deter or penalize protected expression or association" or the inadequacy of the plaintiffs' allegations of freedom of association burden alone is sufficient to overcome the claim of freedom of association infringement. The government's argument must stand or fall on its claims about the program's tailored use of the data.

Plaintiffs' members, their clients, or anyone else with whom they associate; do not allow the Government to scrutinize their contacts indiscriminately; and have no alleged purpose other than the concededly compelling interest of identifying terrorist operatives and preventing terrorist attacks."

The government's contention that it does not acquire associational membership lists when it collects telephony metadata in bulk is unconvincing. There is no question that the telephony metadata can be used to infer associational membership, at least approximately, and that the NSA is developing and using social network analysis tools for that purpose.[97] Either the metadata can be used to determine membership in terrorist networks, in which case it also can be used to determine membership in legitimate associations, or it cannot, in which case it is not serving the compelling government interest that assertedly justifies its collection.[98] The technical possibility of obtaining associational membership information by collecting metadata, rather than by demanding a list, should not be permitted to circumvent basic freedom of association guarantees any more than, in the Fourth Amendment context, the thermal imaging of the interior of a home should be treated simply as collection of infrared radiation in "plain view" outside the home.[99] If the metadata can be used to derive membership lists for an untold number of legitimate associations, its collection by government officials burdens freedom of association for precisely the reasons articulated in *Shelton*: when those wielding government power have information about "every conceivable kind of associational tie-social, professional, political,

[97] It is true that the metadata does not contain "names and addresses" corresponding to telephone numbers. Matching telephone numbers to names is usually a trivial matter using publicly available resources. In any event, one assumes that the NSA has that capability or the data would not be of much use for its own purposes.

[98] For some of the reasons discussed in Part II, it is quite possible that the metadata surveillance program is not particularly useful for doing anything more than could be done with properly supported requests for the telephone records of individuals suspected of terrorist affiliations. Indeed, the paucity and nature of publicly disclosed examples of uses of the data, along with the critical comments of members of Congressional intelligence committees suggest that this may be the case. I ignore that possibility here not because it is implausible, but because it would remove any arguable justification for the program. Moreover, as mentioned in the conclusion, technology can be expected to progress. Equally importantly, belief in the "big data" panacea is likely to be with us for some time, making it important to consider not only what is, but what might possibly be.

[99] Kyllo.

avocational, or religious," there is opportunity for abuse of that power or, at a minimum, for chilling effects based on concern about the ramifications of particular associational choices.

The government's contends that there will be no abuse because "the telephony metadata program is conducted for … legitimate purposes of counter-terrorism"[100] and because the requirements of the order authorizing the telephony metadata collection limit the freedom of association burden by controlling the use to which the metadata is put and provide sufficient tailoring of means to ends in light of the value of the program's contribution to the compelling interest of preventing terrorist attacks.[101]

As discussed above in detail, the mere existence of benign purposes is insufficient. Constitutional rights are designed to protect against government over-reaching, whether or not well-intentioned. Thus, "first amendment analysis has always embraced a healthy scrutiny of governmental action, and protected against possible misuse of government power to take reprisals against political activity or expression."[102] To quote again from *Keith*, "security surveillances are especially sensitive because of the inherent vagueness of the domestic security concept, the necessarily broad and continuing nature of intelligence gathering, and the temptation to utilize such surveillances to oversee political dissent." This basic point is no less true of foreign intelligence investigations conducted within U.S. borders. Moreover, "strict scrutiny is necessary even if any deterrent effect on the exercise of First Amendment rights arises, not through direct government action, but indirectly as an unintended but inevitable result of the government's conduct in requiring disclosure."[103]

The program's constitutionality thus rests on whether the Section 215 order's restrictions provide the necessary fit between means and ends while imposing minimal freedom of association burden. The

[100] Reply brief MTD
[101] White Paper
[102] Australia/Eastern USA Shipping Conf. V. United States, 537 F. Supp. 807 (DDC 1982)
[103] Buckley v. Valeo

order[104] permits authorized NSA personal to access the metadata "for purposes of obtaining foreign intelligence information only through queries [] to obtain contact chaining information[105] … using selection terms" that meet the reasonable articulable suspicion standard. NSA analysts may use the metadata extracted by these queries with few restrictions. The extracted data is placed in a "corporate store," which may "be searched by appropriately and adequately trained personnel for valid foreign intelligence purposes, without the requirement that those searches use only RAS-approved selection terms." While the NSA must generate an auditable record of access to the metadata, there is no such requirement for searches of the "corporate store." Dissemination of information obtained from the metadata is subject to minimization procedures. In particular, "prior to disseminating any U.S. person identifying information outside NSA, [one of several specified intelligence officials] must determine that the information identifying the U.S. person is in fact related to counterterrorism information and that it is necessary to understand the counterterrorism information or assess its importance."[106]

Internal "oversight" of the NSA's activities under the Section 215 order includes personnel training and monitoring, with periodic consultation on legal issues with appropriate DOJ officials.[107] Oversight by the Court has two parts: (1) monthly reports discussing "NSA's application of the RAS standard, as well as NSA's implementation and operation of the automated query process," stating the number of instances in which NSA has shared query results containing U.S. person information outside of the NSA, and attesting that the requisite determination of relation to counterterrorism information was made in each instance and (2) a requirement that, prior to an application to renew the order, NSA must submit a written report of a meeting of specified NSA representatives to assess compliance with the

[104] Order of October 11, 2013
[105] The unredacted portion of this order does not mention the "three-hop" query limitation, but refers to an "automated query process" initially approved in 2012. According to the Obama Administration August 2013 White Paper, the three-hop limitation remains in place.
[106] FISC Order.
[107] For example, specific NSA and DOJ officials are periodically to "a sample of the justifications for RAS approvals for selection terms used to query" the data.

order, including "a review … to ensure that only approved metadata is being acquired" and a report describing "any significant changes proposed in the way in which the call detail records would be received from the Providers and any significant changes to the controls NSA has in place to store, process, and disseminate" the metadata.

These Court-mandated procedures have numerous weaknesses. First, they do relatively little to cabin the government's discretion. The reasonable articulable suspicion determination is made entirely within the executive branch and, though the NSA must discuss its application of the RAS standard in its reports to the FISC, the NSA's application of the standard to particular query targets, including its application of the ban on finding RAS based solely on First Amendment protected activities of U.S. persons, is completely unreviewable. There is also no opportunity for judicial review of whether these standards, as applied, are sufficiently stringent to meet the First Amendment threshold for the sweeping inquiry into a target individual's affiliations permitted by a three-hop query. The NSA also has complete discretion as to how it uses the metadata graph resulting from a query to uncover associations represented in the data, many of which will not involve the target. Second, the oversight procedures mandated by the FISC do not provide an independent check to ensure that NSA analysts do not target telephone numbers for which no reasonable articulable suspicion determination has been made. The NSA polices itself for such non-compliance incidents and self-reports on them only in classified forums. These weaknesses in the regulation of targeting and use of the metadata leave the NSA with exactly the kind of discretion and potential for mission creep that concerned the Supreme Court in *Keith*.

The Section 215 order's standards also do little to improve the program's fit between means and ends. A three-hop network graph surrounding a properly targeted inquiry can be used to infer membership lists for numerous legitimate associations and lists of numerous innocent individuals'

associational affiliations. Thus, a social network analysis of even a properly targeted analysis is much more intrusive than the disclosure requirement that was struck down in *Shelton*.

The government argues that "the program's objectives could not be achieved … [through targeted collection of] "metadata associated only with the calls of persons already known to be, or suspected of being, terrorist operatives" and that, "without its aggregation of bulk metadata, the NSA's ability to detect previously unknown chains of communications among terrorist operatives, crossing different time periods and provider networks, would be impaired." That is not the proper question. The question is whether the comprehensive collection of telephony metadata advances the compelling interest of ""identifying terrorist operatives and preventing terrorist attacks" sufficiently more than less intrusive alternatives, such as staged acquisition of call data for individuals about whom a requisite level of suspicion is reached.[108] The conclusory statement that "[m]ulti-tiered contact chaining identifies not only the terrorist's direct associates, but also indirect associates, and, therefore provides a more complete picture of those who associate with terrorists and/or are engaged in terrorist activities" says nothing about the program's effectiveness in distinguishing between legitimate and malevolent associations or about burdens imposed on legitimate associations by false positive identifications.

Publicly available evidence as to the effectiveness of the metadata surveillance program is thin and does not specify the extent to which reported successes could have been achieved with less comprehensive data collection and analysis. In affidavits filed in *ACLU v. Clapper*, government officials make various claims about the program's efficacy and relate anecdotal examples of its use.[109] Most of those claims do not appear to rely either on comprehensive metadata acquisition or on two or three-hop social network analysis and it seems likely that single-hop call records of phones associated with suspected terrorists could be used to produce equivalent information with only somewhat more effort.

[108] See, e.g., Strandburg; Leahy bill
[109] Cite to affidavits

The government's arguments for comprehensive metadata collection indirectly support this intuition. The government provides three such reasons: 1) avoiding delay (i.e. "[a]ny other means that might be used to attempt to conduct similar analyses would require multiple, time-consuming steps that would frustrate needed rapid analysis in emergent situations"); 2) facilitating aggregation of data from various service providers; and 3) access to historical metadata records "given that terrorist operatives often lie dormant for long periods of time." The upshot of the first two justifications is that it is more efficient for the NSA to have the data at its fingertips than to have to make separate queries based on individual assessments of relevance. Only the last justification suggests any substantive advantage of comprehensive metadata collection and it is clear neither how significant the need for historical records is nor how much the NSA's collection adds to the retention practices of service providers.[110] In any event, none of these justifications is tailored to a particular national security investigation or even to national security generally. Undoubtedly, one could argue that government acquisition of complete historical records of every individual's associations would be useful for law enforcement and counterterrorism efforts, as would complete records of their locations, their transactions and their conversations. The convenience of total surveillance is not a sufficient justification.

In sum, publicly available evidence provides no basis for assessing whether the *degree* to which comprehensive metadata collection advances counter-terrorism efforts justifies the government's acquisition of and discretionary access to records from which thousands of associational membership lists can be derived. In addition, the oversight procedures set up by Section 215 and by the FISA court's orders do not demand, or even facilitate, the type of scrutiny that the First Amendment's protections for freedom of association require.

## V. Freedom of Association Specificity in a Big Data World

[110] Cite re AT&T maintenance of 25 years of telephony metadata.

Technological and societal developments have led to an ever-increasing role for digitally intermediated social interactions. Along with increases in computational speed and cheap data storage, the data trails left by those societal trends drive a tendency to view data analysis as a panacea approach to solving society's problems.[111] Strong, and sometimes extravagant, claims about big data's revolutionary potential are common. Big data optimism fuels attempts by everyone from industry to researchers to governments to create, acquire and store more and more data. This cycle has brought us to a crossroads for freedom of association. Current doctrine imagines that government obtains an association's membership list by first identifying an organization and then requesting membership information either directly or from a third party intermediary using a court order or subpoena. If disclosure is challenged, doctrinal analysis proceeds sequentially by determining whether the organization is an "expressive association," then, at least in some courts, by assessing whether there is a "prima facie case" of a freedom of association burden, then by determining whether the government has put forth a compelling interest in acquiring the information, and finally by analyzing whether that interest could be "achieved through means significantly less restrictive of associational freedoms."[112]

Metadata surveillance circumvents this standard analysis. Government officials plausibly, and perhaps truthfully, claim a complete disinterest in investigating legitimate associations. Yet, the very purpose of subjecting metadata to social network analysis and other data mining techniques is to produce associational membership lists. While the goal may be to attain a list of members of a terrorist network or other malevolent organization, network analysis is indiscriminate. It unavoidably produces (approximate) membership information for legitimate and malevolent associations alike.[113] Whether a

[111] See, e.g., Gil Press, A Very Short History of Big Data, Forbes (May 9, 2013)
[112] Boy Scouts v. Dale.
[113] The fact that the membership list is identified by telephone number, rather than name, is immaterial, given the widespread availability of data connecting telephone numbers to names.

particular cluster corresponds to an expressive association can be determined only after the proverbial horse is out of the barn and the association's membership list is in the government's hands.

There are two possible avenues toward restoring meaningful freedom of association in the current technosocial milieu. First, metadata collection can be regulated to require a closer nexus to compelling governments such as counterterrorism and law enforcement. In my 2008 article, for example, I suggested a staged approach in which at each hop metadata is collected only for those individuals about whom there is a requisite level of suspicion provided by further investigation. The Intelligence Oversight and Reform Act recently proposed by Senators Wyden, Udall, Blumenthal and Paul takes a similar approach, though it permits court orders for data that is within two hops of any "suspected agent of a foreign power who is the subject of such investigation." The proposed bill also provides authority for the Attorney General to compel disclosure of such records without a court order in emergency situations. Second, procedures can be put in place to decrease the discretion afforded to law enforcement and intelligence officials and increase their accountability.[114] The Intelligence Oversight and Reform Act takes some steps in this direction, for example by creating a role for constitutional advocacy before the FISA court. Such reforms should be developed and evaluated with the specificity requirements of the First Amendment's freedom of association guarantee in mind.

[114] See Rascoff.

Preliminary Draft – Please Do Not Cite Without Permission
To be Published in *I/S: A Journal of Law and Policy for the Information Society*
9 ISJLP ___ (2014).
http://www.is-journal.org

# *National Insecurity: The Impacts of Illegal Disclosures of Classified Information*

Mark D. Young*

> There had never been anything like it. In today's terms, it was as if an NSA employee had publicly revealed the complete communications intelligence operations of the Agency for the past twelve years-all its techniques and major successes, its organizational structure and budget-and had, for good measure, included actual intercepts, decrypts, and translations of the communications not only of our adversaries but of our allies as well.[1]

In the mid-summer of 2013, the British newspaper, *The Guardian*, published claims by a contractor for the National Security Agency (NSA) that millions of telephone records were being collected under an order from the Foreign Intelligence Surveillance Court. Throughout the summer, additional disclosures about apparent surveillance operations seized headlines around the world. Interpreting the meaning of the disclosures has been more complicated, but it is clear that there is great interest in United States intelligence activities.

Despite being fired from his contractor position with Booz Allen Hamilton[2] and charged with espionage and theft, Edward Snowden continued to provide classified information to *The Guardian*. The paper has published more than 300 stories on signals intelligence methodologies, the statutes and court authorities under which the United States Intelligence Community conducts these operations, and the intelligence relationships between foreign governments and the United States.[3]

These disclosures of sensitive and classified information concern not only the United States, but also its allies. The material disclosed by Snowden has implicated the United Kingdom's Government Communications Head Quarters (GCHQ). British government concerns about the potential publication of classified data were significant enough to threaten *The Guardian* with legal action if the information was not destroyed. The threats prompted the destruction of hard drives containing information related to GCHQ.[4]

---

*Mark D. Young is the President and General Counsel of Ronin Analytics, LLC. Previously he served as the Executive Director for the Directorate of Plans and Policy at United States Cyber Command, the Special Counsel for Defense Intelligence for the House Permanent Select Committee on Intelligence, and as a senior leader at the National Security Agency. The views expressed in this article are those of the author and do not reflect the official policy or position of the U.S. government. This article is derived entirely from open source material and contains no classified information.

[1] National Security Agency, "The Many Lives of Herbert O. Yardley," *Crytptologic Spectrum* (Autumn 1981, 12) at

10.

[2] http://articles.latimes.com/2013/jun/11/news/la-pn-edward-snowden-fired-booz-allen-20130611

[3] http://www.theguardian.com/world/2013/aug/21/edward-snowden-nsa-files-revelations

[4] Julian Borger, "NSA files: why the Guardian in London destroyed hard drives of leaked files," The Guardian August 20, 2013 available at http://www.theguardian.com/world/2013/aug/20/nsa-snowden-files-drives-destroyed-

The national security implications of the disclosure of this information are significant. According to the most experienced U.S. intelligence officer, Michael V. Hayden,[5] "Edward Snowden will likely prove to be the most costly leaker of America secrets in the history of the Republic."[6] The Chairman of the House Intelligence Committee has noted that Snowden has jeopardized U.S. national Security" by exposing on-going U.S. counterterrorism activities.[7] The Director of National Intelligence stated, "The unauthorized disclosure of a top secret U.S. court document threatens potentially long-lasting and irreversible harm to our ability to identify and respond to the many threats facing our nation."[8]

Snowden claims that his disclosures – in violation of law, regulation, and his solemn oath – are motivated by his judgment about the value of the intelligence. He removed and released data that allegedly shows how the National Security Agency had collected information on civilian institutions, to include universities, hospitals, and businesses. Snowden claims these alleged NSA operations are dangerous and criminal: "These nakedly, aggressively criminal acts are wrong no matter the target."[9] Without referencing the multiple layers of intelligence oversight within the Department of Defense, the Office of the Director of National Intelligence, the National Security Agency's Inspector General, and the Intelligence Community Inspector General, Snowden concluded that "the public needs to know the kinds of things a government does in its name, or the "consent of the governed" is meaningless."[10]

Regardless of one's sympathy for Snowden's conclusion, the scope and scale of the material he has revealed will continue to have a significant impact on United States national security. There are four areas where his actions will diminish national security. First, the disclosure of the programs, relationships, and operations will facilitate operational changes in the behavior of adversarial groups such as al-Qaida and Hamas.[11]It will become more difficult, more expensive, and more time consuming to collect and analyze information on terrorist groups, foreign governments, and foreign militaries.

Second, the disclosures will complicate U.S. foreign relations that directly contribute to U.S. security interests. Cooperation between U.S. and foreign intelligence organizations is critical to the security of the U.S.[12] Other countries are perpetually concerned about disclosing sensitive

---

london. This destruction has not prevented the further disclosures of classified data, however, since the reporter who first broke the story, had additional copies of the material in Brazil and in the United States (http://www.theguardian.com/world/2013/aug/20/nsa-david-miranda-guardian-hard-drives).

[5] General Michael V. Hayden is a career military intelligence officer who led the Central Intelligence Agency, the National Security Agency, and was the first Principal Deputy Director of National Intelligence.

[6] http://www.cnn.com/2013/07/19/opinion/hayden-snowden-impact/index.html

[7] Rogers Video, http://www.mediaite.com/tv/gop-rep-rogers-blasts-snowden-just-go-to-north-korea-iran-to-round-out-government-oppression-tour/

[8] ODNI, DNI Statement on Recent Unauthorized Disclosures of Classified Information June 6, 2013

[9] Edward Snowden: NSA whistleblower answers reader questions, http://www.theguardian.com/world/2013/jun/17/edward-snowden-nsa-files-whistleblower

[10] Edward Snowden: NSA whistleblower answers reader questions, http://www.theguardian.com/world/2013/jun/17/edward-snowden-nsa-files-whistleblower

[11] See generally "Country reports on terrorism". U.S. State Dept. May 27, 2005. Archived from the original on May 11, 2005. Retrieved 2008-01.26.

[12] The National Strategy for Information Sharing and Safeguarding (December 2012) highlights the importance of sharing with partner nations, "our national security depends upon an ability to make information easily accessible to

information collected by their intelligence services at great expense and effort. Snowden has now exacerbated these concerns and weakened traditionally strong American assurances that information provided to the U.S. will be well protected with little risk of embarrassment or compromise to the providing country. It will become more difficult to cooperate with these partners when there is a stream of evidence that shows that the United States cannot keep a secret.

Third, Snowden's actions have impaired cooperation between the United States government and the U.S. private sector. It was already challenging to share information between the U.S. public and private sectors[13], but the exposure of alleged relationships – whether voluntary or pursuant to a court order - between companies such as Verizon, Google, and Facebook has made corporate entities recoil from the government in fear of a diminished reputation or decline in stock value.

Finally, despite Snowden's claimed objective of exposing an "architecture of oppression"[14] his violation of law, regulation, and oath has eroded the confidence of the American public he was hoping to inform. In our representative democracy, this loss of public confidence will quickly transform into fewer resources for the very departments and agencies that safeguard America. Less authority and more oversight are sure to follow. It is understandable, but the reduction in funding, authority and the increase in oversight are the type of emotionally satisfying reactions that will undermine U.S. national security.

These four consequences of Snowden's illegal exposures of classified data will diminish U.S. national security particularly in the short term. It is possible that the reforms and examination of technical collection and analysis will become stronger in the long term, but this is unlikely in the context of rapidly diminishing government funding, continuing economic hardships, and in an environment in which national security may not be in the forefront of the minds of U.S. citizens.

The current administration's National Security Strategy, published in May 2010 provides the focus for an examination of the impacts of the Snowden disclosures.[15] This strategy prioritizes American leadership by "shaping an international order that can meet the challenges of our time" and "recognizes the fundamental connection between our national security, our national competitiveness, resilience, and moral example."[16] U.S. national security interests are: Strengthening Security and Resilience at Home, the Disruption, Dismantling, and Defeat of Al-Qa'ida and its Violent Extremist Affiliates, the Use of Force only as a last resort, the Reverse the Spread of Nuclear and Biological Weapons, the Advancement of Peace, Security, and Opportunity in the Greater Middle East, the Investment in the Capacity of Strong and Capable Partners, and the Securing of Cyberspace.

---

Federal, state, local, tribal, territorial, private sector, and foreign partners in a trusted manner, given the appropriate mission context." Page 7

[13] See generally, Jennifer Martinez and Ramsey Cox "Senate votes down Lieberman, Collins Cybersecurity Act a second time," The Hill November 14, 2012 available at http://thehill.com/blogs/hillicon-valley/technology/268053-senate-rejects-cybersecurity-act-for-second-time.

[14] Video, First Interview at around 7:00, http://www.theguardian.com/world/video/2013/jun/09/nsa-whistleblower-edward-snowden-interview-video

[15] National Security Strategy (2010), available at http://www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf

[16] NSS at 1.

Consistent with the U.S. national security interests are the global and regional threats outlined by the Director of National Intelligence in April 2013. The Increasing Risk to US Critical Infrastructure, Eroding US Economic and National Security, and Information Control and Internet Governance put cybersecurity at the top of the DNI's Worldwide Threat Assessment.[17] Terrorism and Transnational Organized Crime, and the proliferation of weapons of mass destruction were also listed as global threats. With respect to regional threats, Middle East and North Africa (Egypt, Syria, Iran, Iraq, Yemen, Lebanon, and Libya) were listed as threats because the transitioning governments within this region are at risk of failing to "address public demands for change" and "are likely to revive unrest and heighten the appeal of authoritarian or extremist solutions."[18] The information disclosed by Snowden is negatively affecting the national security community's ability to collect and analyze information concerning each of these regional and transnational threats.

**Operational Shifts**

> "Discussing programs like this publicly will have an impact on the behavior of our adversaries and make it more difficult for us to understand their intentions."[19]

The classified material published by the Guardian and other media describes in significant detail the methodologies apparently employed by the National Security Agency in the conduct of its mission. Established in 1952, NSA produces signals intelligence[20] and protects U.S. communications from interception. According to David Kahn, "In intelligence, [NSA] intercepts, traffic-analyzes, and cryptoanalyzes the messages of other nations, friend as well as foe."[21] In addition, NSA executes "the responsibilities of the Secretary of Defense as executive agent for the communications security of the United States Government."[22] This means that the Agency must provide technical and practical means to ensure that no other parties can benefit from the collection of U.S. communications.

Examples of NSA's contributions to national security are difficult to find because of the sensitivity of the Agency's mission. In recent congressional testimony, however, the Director of National Intelligence said that SIGINT is the primary contributor to counterterrorism intelligence and that multiple empirical studies have shown that signal intelligence, provided by NSA, is the major contributor to answering the hardest intelligence challenges faced by the United States.[23]

---

[17] James R. Clapper, Director of National Intelligence, Worldwide Threat Assessment of the US Intelligence Community Statement for the Record before the House Permanent Select Committee on Intelligence (April 11, 2013) 3 available at http://www.dni.gov/files/documents/Intelligence%20Reports/2013%20WWTA%20US%20IC%20SFR%20%20HPSCI%2011%20Apr%202013.pdf.

[18] Worldwide Threat Assessment at 14.

[19] ODNI DNI Statement on recent …

[20] Intelligence comprising communications intelligence, electronic intelligence, and foreign instrumentation signals intelligence.

[21] David Kahn, The Code Breakers: The Comprehensive History of Secret Communication from Ancient Times to the Internet 675 (Second edition, 1996)

[22] Exec. Order No. 12,333, as amended.

[23] USHR19 Joint Committee on Homeland Security , October 29 questioning by Rep. Thornberry to DNI Clapper at 4:36 available at http://www.ustream.tv/recorded/40304984.

Although the claims in the books are unconfirmed, publications such as *Counter Strike: The Untold Story of America's Secret Campaign Against Al Qaeda* by Eric Schmitt and Thom Shanker and *Operation Dark Heart; Spycraft and Special Ops on the Frontlines of Afghanistan – and the Path to Victory* by Lieutenant Colonel Anthony Shaffer suggest that NSA may have prevented significant terrorist attacks and provided critical intelligence during U.S. military operations.

These books, together with the claims of senior intelligence officials before Congress, strongly suggest that NSA's efforts are the most effective shield against the acts of violence to harm Americans and our national security interests. In response to apparent disclosures of NSA activities, President Obama directed the declassification of sensitive NSA collection conducted under the Foreign Intelligence Surveillance Act (FISA). In September 2013, multiple documents concerning "bulk telephony metadata" collection under Section 501 of FISA were declassified and publically released by the Office of the Director of National Intelligence.[24] These disclosures included a Foreign Intelligence Surveillance Court finding of reasonable grounds that the call records were relevant to an authorized terrorism investigation.[25] The same order required NSA to establish "mandatory procedures strictly to control access to and use of the archived data collected pursuant to [the court's] order." Additionally, the order mandated that NSA's General Counsel monitor the designation of those with access to the data and act as an approval authority for the actual queries analysts wished to make of the data.[26]

In late October 2013, the ODNI released a number of additional documents related to NSA's alleged collection programs. These documents include a 2009 congressional notification describing the failure to comply with a Foreign Intelligence Surveillance Court order,[27] and a March 2009 Internal NSA Memorandum of Understanding required for access and query privileges of data collected through NSA's bulk telephony metadata program.[28] These documents describe the legal justifications for and technical detail about how the National Security Agency collects and uses intelligence.

---

[24] Office of the Director of National Intelligence, DNI Clapper Declassifies Additional Intelligence Community Documents Regarding Collection Under Section 501 of the Foreign Intelligence Surveillance Act (October 28, 2013) available at http://www.dni.gov/index.php/newsroom/press-releases/191-press-releases-2013/954-dni-clapper-declassifies-additional-intelligence-community-documents-regarding-collection-under-section-501-of-the-foreign-intelligence-surveillance-act. FISA Section 501 was amended by Section 215 of the USA PATRIOT Act (Section 215) in 2001. P.L. 107-56?

[25] FISA Ct., Order In Re Application of the Federal Bureau of Investigation for An Order Requiring The Production of Tangible Things From____, at 3 Docket No. BR 06-05 available at http://www.dni.gov/files/documents/section/pub_May%2024%202006%20Order%20from%20FISC.pdf

[26] FISA Ct., Order In Re Application of the Federal Bureau of Investigation for An Order Requiring The Production of Tangible Things From____, at 5-6 Docket No. BR 06-05 available at http://www.dni.gov/files/documents/section/pub_May%2024%202006%20Order%20from%20FISC.pdf

[27] National Security Agency, Memorandum for the Staff Director, House Permanent Select Committee on Intelligence, Congressional Notification: Incidents of Noncompliance – Information memorandum (February 25, 2009) available at http://www.dni.gov/files/documents/501/25%20Feb%2009%20NSA%20CN_SealedFINAL.pdf.

[28] Available at http://www.dni.gov/files/documents/501/Mem%20of%20Understanding%20for%20H2I4%20HMCs_Sealed%20FINAL.pdf

This information was declassified and publically released to inform the public about what data were collected and analyze by NSA, to balance inaccurate speculations by the media about NSA, and to facilitate the debate about U.S. intelligence Community operations. When examined together, the information disclosed by Snowden and the declassified information released by the ODNI present a positive picture of prudent measures for national security. If the information about programs such as PRISM, FAIRVIEW, or OAKSTAR is accurate, then it appears as if the intelligence community has not only adjusted well to global technical advancements in telecommunications, but also learned significant lessons from the September 11, 2001 terrorist attacks.

It was known in early 2001 that NSA's effectiveness was challenged by the "multiplicity of new types of communications links, by the widespread availability of low-cost encryption systems, and by changes in the international environment in which dangerous security threats can come from small, but well organized, terrorist groups as well as hostile nation states."[29] Any challenge about the value of an intelligence program must address the importance of data quantity and quality. First, since intelligence analysis depends on having access to relevant information, logic dictates that more data is always better. As noted by Mark Lowenthal:

> The issue then becomes how to extract the intelligence from the mountain of information. One answer would be to increase the number of analysts who deal with the incoming intelligence, but that raises further demands on the budget. Another possible response, even less palatable, would be to collect less. But, even then, there would be no assurance that the "wheat" remained in the smaller volume still being collected.[30]

Thus, quantity has an intelligence quality all its own. In addition, the type of information needed by the intelligence community is also important. Given the priorities noted in the National Security Strategy, the importance of NSA collection and analysis as noted in congressional testimony and the ever-present threats by terrorist groups and hostile nations the American public should vigorously endorse the type of programs viewed by Snowden as oppressive. It is troubling to see the disclosure of techniques allegedly used by NSA to obtain "cryptographic details of commercial cryptographic information security systems through industry relationships,"[31] and the rampant speculation about the monitoring of the mobile phones of the heads of state from Europe.

It is not only logic that leads one to believe in the value of NSA collection, but also testimony by intelligence professionals. For example, according to the House Intelligence Committee, NSA activities have "been integral in preventing multiple terrorist attacks, including a plot to attack on the New York Stock Exchange in 2009."[32] The PRISM program – a program reported to provide

---

[29] Richard A. Best, Jr., *The National Security Agency: Issues for Congress* 1 Congressional Research Service January 16, 2001 available at http://www.fas.org/irp/crs/RL30740.pdf.
[30] Mark M. Lowenthal, *Intelligence: From Secrets to Policy* 55 (2000).
[31] theguardian.com, "NSA: classification guide for cryptanalysis" 5 September 2013 available at http://www.theguardian.com/world/interactive/2013/sep/05/nsa-classification-guide-cryptanalysis
[32] HPSCI Urge of support for NSA, http://intelligence.house.gov/press-release/chairman-mike-rogers-and-ranking-member-dutch-ruppersberger-urge-support-important-nsa.

NSA access to information some of the largest technology companies - provided "critical leads" to disrupt more than 50 potential terrorist events in more than 20 countries. The Foreign Intelligence surveillance Act authority - the congressional authorization to target communications of foreign persons who are located abroad for foreign intelligence purposes - contributed to more than 90 percent of these disruptions.[33]

The Deputy Attorney General has noted that the Federal Bureau of Investigation benefited from NSA's Section 702 collection in the fall of 2009. Using Section 702 collection and "while monitoring the activities of Al Qaeda terrorists in Pakistan, the National Security Agency (NSA) noted contact from an individual in the U.S. that the Federal Bureau of Investigation (FBI) subsequently identified as Colorado-based Najibulla Zazi. The U.S. Intelligence Community, including the FBI and NSA, worked in concert to determine his relationship with Al Qaeda, as well as identify any foreign or domestic terrorist links."[34]

"The FBI tracked Zazi as he traveled to New York to meet with co-conspirators, where they were planning to conduct a terrorist attack. Zazi and his co-conspirators were subsequently arrested. Zazi, upon indictment, pled guilty to conspiring to bomb the NYC subway system. Compelled collection (authorized under Foreign Intelligence Surveillance Act, FISA, Section 702) against foreign terrorists was critical to the discovery and disruption of this threat against the U.S."[35] Regardless of the accuracy of the information released by Snowden, the types of programs described by the material contribute to national security and its released, regardless of its validity will negatively impact US security.

Homegrown Violent Extremists[36] continue to be inspired by global jihadist propaganda and the perceived success of plots such as the November 2009 attack at Fort Hood, Texas and the March 2012 attacks by an al-Qa'ida-inspired extremist in Toulouse, France.[37] The threat from terror groups remains existential and of great concern to the U.S. intelligence community. The revelations concerning the NSA's counterterrorism successes will motivate terror groups to reexamine how they communicate, plan, and execute these attacks.

*Terror Groups*. It is likely t hat terrorist groups will change how they conceive, plan, and execute terrorist attacks as a result of the classified intelligence information now exposed to the public. Terrorist groups continuously adjust their methodologies for attacking their targets[38], but the recent disclosures provide a roadmap for terror groups to avoid detection.

---

[33] HPSCI Open hearing around 37:30 http://www.c-spanvideo.org/program/AgencyOp

[34] HPSCI Web page, http://intelligence.house.gov/1-four-declassified-examples-more-50-attacks-20-countries-thwarted-nsa-collection-under-fisa-section and CSPAN HPSCI Hearing at 39:30

[35] HPSCI Web page, http://intelligence.house.gov/1-four-declassified-examples-more-50-attacks-20-countries-thwarted-nsa-collection-under-fisa-section

[36] *See generally* Jerome P. Bjelopera, American Jihadist Terrorism: Combating a Complex Threat 5 Congressional Research Service (R41416 )(January 23, 2013) (Homegrown violent extremists are jihadist-inspired American citizens or legal permanent residents that plan or conduct terrorist attacks on the United States.) available at http://www.fas.org/sgp/crs/terror/R41416.pdf

[37] WWT SFR at 4

[38] According to the Director of National Intelligence, Al-Qa'ida in the Arabian Peninsula remains focused on attacks on US soil and "continues to adjust its tactics, techniques and procedures for targeting the West." (WWT at 3)

As similar example of how terrorist groups adjust their planning and communication techniques in response to the disclosure of classified information is found in the 9/11 Commission report. Referring to a 1998 *Washington Times* story disclosing that Osama Bin Laden communicated with a satellite phone, the 9/11 Commission noted that al Qaeda's senior leadership "had stopped using a particular means of communication almost immediately after a leak to *The Washington Times*. This made it much more difficult for the National Security Agency to intercept his conversations."[39] Despite the controversy surrounding this story, it makes logical sense that terror groups will not use technologies reportedly monitored by those who seek to disrupt their plans.

Similar changes in terror group practices as reported by the *New York Times* can be anticipated with the Snowden disclosures. The details of how intelligence targets will alter their practices are speculative given the obscurity of terrorist methodologies, but a few points are clear.

If the reports are true and NSA can exploit[40] the "worldwide use of nine U.S.-based Internet service providers, including Google, Yahoo, Skype and YouTube," then it is reasonable to assume that terrorist groups using these technologies or services will discontinue use of these services. According to the *New York Times*, the Snowden disclosures resulted in jihadists posting Arabic news articles about [NSA's capabilities] … and recommended fellow jihadists to be very cautious, not to give their real phone number and other such information when registering for a website." [41] Similar posts recommending jihadists use "privacy-protecting email systems like The Onion Router, to hide their computer's IP address, and to use encrypted links to access jihadi forums"[42] provide direct evidence that the recent disclosures will change how terrorists plan and conduct their attacks.

Another example concerns alleged NSA access to Skype. Purchased by Microsoft in 2011, Skype claims to employ standard encryption to protect users from hackers and criminals.[43] Documents published by the Guardian suggest that NSA may have had access to Skype servers.[44] Despite this suggested access, others claim that Skype calls made to other Skype customers were untraceable because of Skype corporate location. "Skype is located in Luxembourg (outside of the United States), and…[encryption] keys used by Skype cannot be turned over to the FBI because Skype does not hold the keys themselves. The key is only known by the computers using the program to connect with each other, and Internet communication is inherently hard to trace because of how packets can be routed."[45]

---

[39] 9/11 Commission report at 127

[40] Taking full advantage of any information that has come to hand for tactical, operational, or strategic purposes. (JP 1-02 at 96)

[41] http://nypost.com/2013/06/26/terrorists-to-ditch-skype-and-youtube-after-leaks-reveal-nsa-surveillance-tactics/

[42] http://nypost.com/2013/06/26/terrorists-to-ditch-skype-and-youtube-after-leaks-reveal-nsa-surveillance-tactics/

[43] http://www.skype.com/en/security/#encryption (Inaccessible as of 11/17; use https://support.skype.com/en/faq/FA31/does-skype-use-encryption?frompage=search&q=encryption&fromSearchFirstPage=false)

[44] NSA Prism program slides, The Guardian, 1 November 2013 available at http://www.theguardian.com/world/interactive/2013/nov/01/prism-slides-nsa-document

[45] http://www.unitedliberty.org/articles/talk-like-a-terrorist-use-skype (However, see http://www.nytimes.com/2013/09/06/us/nsa-foils-much-internet-encryption.html?hp&pagewanted=all&_r=0).

As early as 2011, reports described how terrorist use of Skype was hindering law enforcement in India. According to the *Times of India*, "Terrorist organizations targeting India have moved their communications significantly to Internet and other possible innovative means, denying Indian intelligence agencies any major breakthrough yet in their post-Mumbai blasts investigations." [46] Kashmiri terrorists are reportedly using smart phones and Skype according to a senior Indian Army officer. Terrorists, like the general population, migrate to technologies that enhance communications. The popularity and proliferation of Skype supports the hypothesis that international terror groups have used Skype.

Regardless of the validity of the reports of NSA access to Skype servers or the inability of access to Skype communications, the new attention to alleged Skype vulnerabilities will encourage illicit users to move to other technologies. By exposing real or imagined capabilities of the U.S. Intelligence Community, potential state and non-state targets of electronic surveillance are better equipped to avoid surveillance by avoiding specific technologies and technical services.

One such service is the Society for Worldwide Interbank Financial Telecommunications (SWIFT) network. SWIFT, a member-owned cooperative, enables the standardized exchange of proprietary financial data such as payments, securities, and bank commodity trades.[47] Financial transactions, such as those facilitated by SWIFT, are a direct concern to counterterrorism officials. The 9/11 Commission noted, "Vigorous efforts to track terrorist financing must remain front and center in U.S. counterterrorism efforts. The government has recognized that information about terrorist money helps us understand their network, search them out, and disrupt their operations."[48]

In support of this understanding, an intergovernmental policymaking group established to address money laundering issues in 1989, expanded its mission to include "identifying sources and methods of terrorist financing and adopted nine special recommendations on terrorist financing to track terrorists' funds."[49] The Financial Action Task Force on Money Laundering, comprised of 36 member countries, was develops and promotes "policies to combat money laundering and terrorist financing."

Because terror financing became a priority well before September 11, 2001 the European Union and U.S. began to permit US agencies "limited access to bank data transferred through the SWIFT network." The agreement supported the US Terrorist Finance Tracking Program established after the September 11 attacks.[50] Recent disclosures have focused attention on the data reportedly accessed by NSA.

---

[46] http://articles.timesofindia.indiatimes.com/2011-07-19/india/29790655_1_satellite-phones-intelligence-agencies-thuraya

[47] See generally SWIFT Company information available at http://www.swift.com/about_swift/company_information/company_information and "FIN traffic "available at http://www.swift.com/assets/swift_com/documents/about_swift/SIF_2013_09.pdf

[48] 9/11 Commission report at 382.

[49] James K. Jackson, The Financial Action Task Force: An Overview at "Summary" May 9, 2012 (CRS)( RS21904) available at http://www.fas.org/sgp/crs/misc/RS21904.pdf

[50] JERIN MATHEW, "Edward Snowden NSA Scandal: EU to Suspend US Data Sharing After Swift's Interbank Messaging System Breach," International Business Times (September 25, 2013) available at http://www.ibtimes.co.uk/articles/508882/20130925/edward-snowden-nsa-scandal-swift-tftp-eu.htm

In response to this arrangement being made public, the European Union has threatened to "suspend or even terminate the crucial EU-US Terrorist Finance Tracking Programme."[51] The national security impact of this disclosure is the potential loss of an apparently valued source of financial intelligence.[52] The importance of terrorist financing is self-evident. If, pursuant to an international agreement, NSA had access to international money transfers, it is reasonable to believe that U.S. intelligence community was well positioned to interdict the planning and execution of violent actions against the U.S. of her allies. If financial transfers are moved as a result of the illicit disclosures of collection of networks such as SWIFT, then U.S. understanding and ability to prevent terrorist actions is significantly degraded.

Snowden's disclosures have already changed terror group's practices making it more difficult for U.S. intelligence agencies to provide warnings about terror groups' plans and intentions. The loss of insight into these targets diminishes U.S. security, but also prevents the U.S. from sharing information with its allies and partners, diminishing U.S. global influence. The net effect of Snowden's disclosures is to increase terrorist consciousness of their own vulnerabilities. Their response has been immediate and may have a dangerous cumulative effect.[53]

**Foreign Relations**

> However the Snowden episode turns out ... what it mainly illustrates is that we are living in an age of American impotence. The Obama administration has decided it wants out from nettlesome foreign entanglements, and now finds itself surprised that it's running out of foreign influence.[54]

Beyond the national security impact of making terrorist intentions and plans harder to discover and the change in practices of terrorist and opposition groups, Snowden's release of classified information will diminish national security by degrading U.S. foreign relations. American security relies heavily on foreign partnerships that have increased in breadth and scope since the September 11, 2001 terrorist attacks.

Foreign governments are likely to share less information and require more scrutiny of future interactions with U.S. intelligence and no country allegedly targeted for collection is pleased to see the public reports about it. Rising anti-Americanism will strain already tense relationships with countries such as Russia and China; European Union officials have expressed outrage over the Snowden disclosures.[55] The reports have already distracted the U.S. and Russian delegations

---

[51] Jerin Mathew , "Edward Snowden NSA Scandal: EU to Suspend US Data Sharing After Swift's Interbank Messaging System Breach," International Business Times (September 25, 2013) available at http://www.ibtimes.co.uk/articles/508882/20130925/edward-snowden-nsa-scandal-swift-tftp-eu.htm

[52] CRS Report, http://www.fas.org/sgp/crs/row/RS22030.pdf

[53] *See generally* Gabriel Schoenfeld, *Necessary Secrets: National Security, the Media, and the Rule of Law* (2010) at 121.

[54] Bret Stephens, "The Age of American Impotence," Wall Street Journal June 25, 2013 available at http://online.wsj.com/news/articles/SB10001424127887324637504578565530512048940

[55] http://www.usatoday.com/story/theoval/2013/07/04/obama-merkel-snowden-surveillance-leaks/2488927/

during the August 2013 G-20 Summit in Russia during which tensions about Snowden's extradition and asylum status were unresolved.[56]

In addition to diplomatic relationships, United States' intelligence agencies have extensive relationships with foreign intelligence services. Not only will diplomatic interactions be more difficult, but the intelligence relationships will be challenges as well. U.S. intelligence has good relations with many foreign intelligence services despite what one may read in the press during periods of heightened intelligence interest.

The Director of National Intelligence has the authority to establish intelligence arrangements with foreign governments.[57] The Director of the Central Intelligence Agency has a mandate to "conduct foreign intelligence liaison relationships with intelligence or security services of foreign governments or international organizations…."[58] The Director of the Defense Intelligence Agency is also required to "conduct foreign defense intelligence liaison relationships and defense intelligence exchange programs with foreign defense establishments, intelligence or security services of foreign governments…."[59] The Director of the National Security Agency has a similar mandate: The Director of the National Security Agency shall "conduct foreign cryptologic liaison relationships…."[60]

Each of these mandated liaison relationships will likely suffer because of the recent disclosures. These relationships can sour if foreign public opinion becomes dissatisfied with U.S. activities that may occur in secret, but with the approval of other heads of state.

*Russia*. The disclosure of alleged intelligence collection may have shifted the balance of moral authority toward Moscow as global awareness of the reported NSA programs proliferated. Russian President Vladimir Putin has been emboldened by the Snowden revelations as illustrated by his actions concerning Syria since the first release of data by *the Guardian* on June 5, 2013.

Russia's goal in Syria before the release of the classified information was avoid a "Western-backed effort at coercive regime change."[61] Russia has been anxious about the popularity of Islamist groups in predominantly Sunni Muslim countries after the Arab Spring revolutions.[62] Russia attributes the growth of these groups to U.S. attempts to spread democracy throughout the Middle East.[63] Thus, President Putin's political motivations have traditionally been more about domestic stability than about expanding Russia's foreign influence.[64] There was much

---

[56] See generally http://www.cnbc.com/id/100989042 and http://www.cbsnews.com/8301-250_162-57596558/obama-reevaluating-summit-with-russia-after-snowden-asylum/

[57] EO12333, Section 1.3(b)(4)(A)

[58] EO12333 Section 1.7(a)(5)

[59] EO12333 Section 1.7 (b)(5)

[60] EO12333 Section 1.7 (c)(8)

[61] Samuel Charap and Jeremy Shapiro, "How the US Can Move Russia on Syria," Al-Monitor, (July 22, 2013) available at http://www.al-monitor.com/pulse/originals/2013/07/syria-russia-geneva-engagement-peace-process-us-interests.html

[62] Fiona Hill, The Survivalist in the Kremlin, Project Syndicate (Jul. 4, 2013) available at http://www.project-syndicate.org/commentary/putin-s-rigid-approach-to-protecting-russia-by-fiona-hill

[63] Fiona Hill.

[64] According to Brookings Institute Senior Fellow Cliff Gaddy, "The whole point of their policy on Syria is that they are trying to protect themselves. What they are afraid of is instability. … Not really caring that much about who is in

speculation about how the events in Syria would be addressed by the G-20 summit. Analysts reported that Putin may not engage the topic. "He may not even, at the summit, engage in any major rhetorical condemnation of [chemical weapons use in Syria]. I think he may just let it, let the events speak for themselves."[65]

Despite this anxiety, Russia was relatively subdued on Syria until after the Snowden revelations. Emboldened by the growing global discontent with the U.S., Putin became more vocal on Syria and on U.S. foreign policy. His most dramatic maneuver was to publish an opinion article in the New York Times on September 11, 2013. According to Fiona Hill, of the Brookings Institute:

> Russian President Vladimir Putin has done it again, grabbing American and international attention with his *New York Times* op-ed cautioning the United States against the use of force in Syria, and scolding America for considering itself exceptional. Putin's piece has been met with surprise and outrage in the U.S., but its basic message has resonated with groups opposed to a unilateral U.S. strike against regime of Syrian President Bashar al-Assad. Putin has put himself right where he wants to be, at the top of the headlines on Syria, and writing the script for where the United States will have to take the crisis next: Back to the United Nations.[66]

Other circumstances concerning Syria undoubtedly helped encourage Putin to be more vocal, [67] but Russia is viewed by many as having taken the diplomatic high ground against President Obama's threat of military force. It is not difficult to interpret Putin's emboldened message, since he was considering - and then granted - temporary asylum to Edward Snowden while the debate on Syria was taking shape.

*European Union*. Traditional strong diplomatic and intelligence sharing relationships with members of the European Union have also been strained by revelations of programs allegedly collecting the personal communication of 35 heads of state.[68] These reports of U.S. surveillance

---

power as long as the people in power in the country control the forces within their borders as best they see. ... I don't think that he has a plan [for Syria] but the overall plan is somehow to protect Russia from the bad things that are happening." (http://www.brookings.edu/blogs/brookings-now/posts/2013/08/28-what-will-russia-do-if-us-strikes-syria).

[65] The Brookings Institute, U.S.-RUSSIA REPORTER ROUNDTABLE, 11 (August 29, 2013) available at http://www.brookings.edu/~/media/research/files/interviews/2013/08/29%20us%20russia%20relations/us%20russia%20relations%20g20%20syria%20arms%20control.pdf

[66] Fiona Hill, "Lessons in Communication from Vladimir Putin," msnbc (September 14, 2013) available at http://www.msnbc.com/msnbc/lessons-communication-vladimir-putin#discussions

[67] "F irst came the British parliamentary vote blocking Prime Minister David Cameron's initiative to join any U.S. military assault. Then came U.S. President Barack Obama's decision to put the issue to a vote before a reluctant Congress. The French government announced that -- unlike in Mali -- it would not go it alone in Syria. And United Nations Secretary-General Ban Ki-moon stated that the chemical weapons inspection team he had dispatched to Syria would need time to complete its work before determining whether there was sufficient evidence for the UN to approve the use of force." (http://www.brookings.edu/research/opinions/2013/09/06-putin-scores-syria-hill)

[68] James Ball, The Gurdian, NSA monitored calls of 35 world leaders after US official handed over contacts," (October 24, 2013) available at http://www.theguardian.com/world/2013/oct/24/nsa-surveillance-world-leaders-calls.

in Europe are "eating away at the fabric of trust that is part of the alliance."[69] According to the Council on Foreign Relations Senior Fellow Charles A. Kupchan , there is a direct relationship between the political discomfort with alleged U.S. intelligence collection and European disappointment about the President's inability to better balance security and civil liberties. Kupchan has noted that many Europeans feel that Obama "has failed to deliver on his pledge to clean up some of the excesses left behind by the George W. Bush administration." [70]

German Chancellor Angela Merkel originally defended the apparent intelligence cooperation disclosed by Snowden. She pointed out that Germany had "avoided terrorist attacks thanks to information from allies." But, in the face of new disclosures, she is now discussing limits on intrusions on privacy. Berlin has alluded repeatedly to "Cold War" tactics and has said spying on friends is unacceptable. Her spokesman has said a transatlantic trade deal requires a level of "mutual trust." [71] Chancellor Merkel has been criticized for her apparently feigned indignation about alleged cooperation with the U.S. intelligence community. "Germany has demanded explanations for Snowden's allegations of large-scale spying by the NSA, and by Britain via a programme codenamed 'Tempora', on their allies including Germany and other European Union states, as well as EU institutions and embassies."[72]

The Head of Germany's domestic intelligence has said he knew nothing about the reported NSA surveillance. Opposition parties believe otherwise. They claimed that, because German intelligence activities are coordinated within the Office of the Chancellor, high-level officials must have known about speculative NSA activities. [73] *Der Spiegel* has reported that NSA monitored about 20 million German phone connections and 10 million internet sessions on an average day and 60 million phone connections on above average days.[74] Thus, unconfirmed U.S. intelligence activities are now an issue that will affect German political leadership and the diplomatic and intelligence relationships between Germany and the U.S.

The impact on European Union allies is already seen in the talks being held between EU member states and the US about American surveillance tactics that may have included spying on European allies.[75] President Obama assured Germany that the United States "takes seriously the concerns of our European allies and partners."[76]

---

[69] Council on Foreign Relations, Interview of Charles A. Kupchan "U.S. Spying Casts Shadow Over Atlantic Alliance" October 29, 2013 available at https://secure.www.cfr.org/europe/us-spying-casts-shadow-over-atlantic-alliance/p31745

[70] Council on Foreign Relations, Interview of Charles A. Kupchan "U.S. Spying Casts Shadow Over Atlantic Alliance" October 29, 2013 available at https://secure.www.cfr.org/europe/us-spying-casts-shadow-over-atlantic-alliance/p31745

[71] http://www.sott.net/article/263704-Merkels-public-indignation-a-scam-Snowden-says-Germans-and-other-Western-states-in-bed-with-NSA.

[72] Merkel's public indignation a scam: Snowden says Germans and other Western states in bed with NSA

[73] http://www.sott.net/article/263704-Merkels-public-indignation-a-scam-Snowden-says-Germans-and-other-Western-states-in-bed-with-NSA.

[74] http://www.sott.net/article/263704-Merkels-public-indignation-a-scam-Snowden-says-Germans-and-other-Western-states-in-bed-with-NSA.

[75] http://www.usatoday.com/story/theoval/2013/07/04/obama-merkel-snowden-surveillance-leaks/2488927/

[76] Laura Smith-Spark**,** EU envoys meet over claims of U.S. spying on European allies CNN available at http://www.cnn.com/2013/07/04/world/europe/europe-us-spying/

The initiation of a dialogue between the U.S. and EU Members about intelligence collection and appropriate oversight[77] will also complicate the transatlantic relationship. Restrictions or legislation that shifts standards of privacy and data protection will diminish American and EU security.

*France*. Tensions in the European Union are not only limited to Germany. Although not as vocal, the French government has expressed concerns about U.S. intelligence activity because of the Snowden leaks. In response to allegations that NSA had collected "more than 70 million phone calls in France over a 30-day period," U.S. Ambassador to France Charles Rivkin was called meet with French diplomats.[78] A news release from French President Francois Hollande's office said he expressed his "deep disapproval with regard to these practices" and that "such alleged activities would be unacceptable between allies and friends."[79]

French indignation aside, the disclosures suggest a greater level of French involvement in global electronic surveillance. According to *the Guardian*, the Snowden materials contain high praise for the U.K's GCHQ's French partner, the General Directorate for External Security (DGSE). The French are reported to be a "highly motivated, technically competent partner, who have shown great willingness to engage on [internet protocol] issues, and to work with GCHQ on a 'cooperate and share' basis."[80] French media, too, has reported that DGSE is involved in the alleged collection. In early November, *La Jeune Politique* reported on the strained relations between Washington, D.C. and Paris. An article published by *Le Monde*, "detailed "the nature of the NSA's probing into France and…reported that data on over 70.3 million phone calls and SMS messages had been recorded by the NSA within a 30-day span." These reports "threw diplomatic relations into question and prompted a visit by Secretary of State John Kerry."[81]

American officials also noted the compliance of foreign intelligence services in the collection programs. According to NSA Director Keith B. Alexander, the documents released by Snowden "didn't represent data collected by the NSA or any other U.S. agency and didn't include records from calls within those countries."[82] In congressional testimony, Alexander noted that the data "were instead from a system that contained phone records collected by the U.S. and North Atlantic Treaty Organization countries 'in defense of our countries and in support of military

---

[77] http://www.usatoday.com/story/theoval/2013/07/04/obama-merkel-snowden-surveillance-leaks/2488927/

[78] Ed Payne and Khushbu Shah, "Report: U.S. intercepts French phone calls on a 'massive scale,' CNN October 21, 2013 available at http://www.cnn.com/2013/10/21/world/europe/france-nsa-spying/

[79] Ed Payne and Khushbu Shah, "Report: U.S. intercepts French phone calls on a 'massive scale,' CNN October 21, 2013 available at http://www.cnn.com/2013/10/21/world/europe/france-nsa-spying/

[80] Julian Borger, GCHQ and European spy agencies worked together on mass surveillance, The Guardian, 1 November 2013 available at http://www.theguardian.com/uk-news/2013/nov/01/gchq-europe-spy-agencies-mass-surveillance-snowden

[81] Grace Jamieson, French Intelligence DGSE Implicated in Snowden NSA Leaks *La Jeune Politique* November 9, 2013 available at http://lajeunepolitique.com/2013/11/09/french-intelligence-dgse-implicated-in-snowden-nsa-leaks/

[82] ADAM ENTOUS and SIOBHAN GORMAN, "Europeans Shared Spy Data With U.S," The Wall Street Journal, Oct. 29, 2013 available at http://online.wsj.com/news/articles/SB10001424052702304200804579165653105860502

operations.'"[83] He said the conclusion that the U.S. collected the data is incorrect. "And it's false that it was collected on European citizens. It was neither."[84]

The disclosures – and comments from the U.S. government - put French leaders in a difficult political position. Despite their initial vocal protest of U.S. intelligence activities, now it appears as if the French intelligence services were not only in on the collection, but also provided the data to their American and British partners. According to U.S. Secretary of State John Kerry, "France is one of the U.S.'s closest allies" and that France and the U.S. "work together to protect the security of their citizens."[85] If these claims are accurate, then it is safe to assume the collaboration and sharing of intelligence goes beyond those activities illegally disclosed by Snowden.

Assuming that the French do provide intelligence assistance to and data sharing with NATO, GCHQ, and NSA, the political pressures may be so strong as to curtail that assistance and sharing. If the media reports about French technical collection capability, the positive GCHQ assessment of French intelligence abilities, and General Alexander's statements about the reasons for intelligence relationships are all true, then any reduction in intelligence and data sharing will reduce the effectiveness of French, U.K, EU, NATO, and U.S. intelligence operations. If the current pressures result in less sharing or more restricted information exchanges between France and the U.S., then it is U.S. national security is impacted.

Some predict that the discomfort with the public disclosure of critical intelligence activities will result in the establishment of new norms of intelligence-gathering within the Atlantic Alliance. Rules such as "no snooping on officials above a certain level; or no significant intelligence gathering without informing the intelligence agency of the other side" are being considered.[86] There is current legislation in the European parliament that seeks to "tighten privacy laws and make it more difficult for Europeans to share information with non-European companies like Google and Facebook."[87] This will make intelligence more difficult and more expensive to collect, also impacting U.S. national security.

*Latin America*. Snowden's illegal disclosures have impacted U.S. national security by weakening foreign relations not only with Russia and Europe, but also in Latin America. Threats to U.S. national security from Latin America remain significant. "Economic stagnation, high rates of violent crime and… ruling party efforts to manipulate democratic institutions to consolidate power, and slow recovery from natural disasters are challenging [security measures]."[88]Countries

[83] Adam Entous and Sioban Gorman , "Europeans Shared Spy Data With U.S," The Wall Street Journal, Oct. 29, 2013 available at http://online.wsj.com/news/articles/SB10001424052702304200804579165653105860502
[84] Adam Entous and Sioban Gorman, "Europeans Shared Spy Data With U.S," The Wall Street Journal, Oct. 29, 2013 available at http://online.wsj.com/news/articles/SB10001424052702304200804579165653105860502
[85] Ed Payne and Khushbu Shah, "Report: U.S. intercepts French phone calls on a 'massive scale,' CNN October 21, 2013 available at http://www.cnn.com/2013/10/21/world/europe/france-nsa-spying/
[86] Council on Foreign Relations, Interview of Charles A. Kupchan "U.S. Spying Casts Shadow Over Atlantic Alliance" October 29, 2013 available at https://secure.www.cfr.org/europe/us-spying-casts-shadow-over-atlantic-alliance/p31745.
[87] Council on Foreign Relations, Interview of Charles A. Kupchan "U.S. Spying Casts Shadow Over Atlantic Alliance" October 29, 2013 available at https://secure.www.cfr.org/europe/us-spying-casts-shadow-over-atlantic-alliance/p31745.
[88] WWT at 26.

hostile to the U.S., such as Iran, have been expanding their influence in Latin America and the Caribbean.[89]

Threats from illicit narcotics trafficking emanate primarily from the Western Hemisphere. Mexico and Colombia are source countries for the majority of illegal drugs consumed in the United States, according to the Director of National Intelligence. Illicit trafficking continues to undermine U.S. security. Some of the highest violent crime rates are found in Honduras, El Salvador and Guatemala. "In addition, weak and corrupt institutions in these countries foster permissive environments for gang and criminal activity, limit democratic freedom, encourage systemic corruption, and slow recovery."[90] National security threats are abundant in Latin America, and recent illegal disclosures of classified information will not help diplomatic or intelligence sharing relationships with permissive or corrupt governments.

The disclosures have impacted U.S. national security relationships with Latin America, but particularly Brazil. Good intentions over the past three years to establish a trade deal and Brazilian membership in the UN Security council have been unsuccessful. Brazil's President Dilma Vana Rousseff has stated that each country has much to gain from deepening coordination with the U.S. It is reasonable to assume that given the threats to stability and the illicit narcotics trafficking from Latin America, that the U.S. intelligence Community has a partnership with Brazil. If true, then the disclosures by Snowden will complicate this cooperation. According to the *New York Times*, "Diplomatic ties have also been damaged, and among the results was the decision by Brazil's president, Dilma Rousseff, to postpone a state visit[91] to the United States in protest over revelations that the agency spied on her, her top aides and Brazil's largest company, the oil giant Petrobras."[92] Although an apology[93] may be enough to have a trade deal between the U.S. and Brazil reenergized, other issues continue to strain the relationship between Washington and Brasília.

According to the Council of Foreign Relations, the Snowden scandal, the White House "response to it and President Dilma Rousseff's decision to cancel the state visit has revealed the weakness of the U.S.-Brazil relationship."[94] Snowden's disclosures are now spawning an effort within Latin America to strengthen protections against alleged NSA collection. "According to the AP, Brazilian Foreign Minister Luiz Alberto Figueiredo said, 'We're going to talk with our partners,

---

[89] President Ahmadinejad traveled to the region twice in 2012. Tehran has cultivated ties to leaders of the Venezuelan-led Alliance for the Peoples of our Americas (ALBA) in Bolivia, Cuba, Ecuador, Nicaragua, and Venezuela, and maintains cordial relations with Cuba and Nicaragua. Relations with Tehran offer these governments a way to stake out independent positions on the international issue of Iran, while extracting financial aid and investment for economic and social projects. (WWT at 26)

[90] WWT at 26

[91] Rousseff was due to make a formal state visit to Washington…to meet U.S. President Barack Obama and discuss a possible $4 billion jet-fighter deal, cooperation on oil and biofuels technology, as well as other commercial agreements. (http://www.reuters.com/article/2013/09/04/us-usa-security-snowden-brazil-idUSBRE98314N20130904).

[92] Eric Schmitt and Michael Schmidt, Qaeda Plot Leak Has Undermined U.S. Intelligence, September 29, 2013 available at http://www.nytimes.com/2013/09/30/us/qaeda-plot-leak-has-undermined-us-intelligence.html?pagewanted=all&_r=0.

[93] http://www.reuters.com/article/2013/09/04/us-usa-security-snowden-brazil-idUSBRE98314N20130904.

[94] http://www.cfr.org/brazil/dear-president-dilma/p31379.

including developed and developing nations, to evaluate how they protect themselves and to see what joint measures could be taken in the face of this grave situation.'"[95]

Not only is U.S. national security affected by reactions in Brazil, but U.S. commercial interests as well. According to the LA Times, President Rousseff is "promoting legislation that would require technology companies such as Google and Facebook to store data collected in Brazil on Brazilian soil and therefore submit it to Brazilian law."[96] In addition, Brazil is now planning to develop a secure e-mail system to improve the security of government communications against American spying. Ironically, "President Dilma Rousseff used the secure messaging channel Twitter to make the announcement that she's going to order SERPRO – that country's federal data processing service – to implement a whole-of-government secure e-mail system."[97]

The reaction in Brazil over the illegal disclosures about alleged surveillance illustrates the diplomatic impact of the disclosure of classified information. The relationships with Latin American trade and diplomatic partners will continue to be tense because of the Snowden leaks. Snowden's actions will continue to degrade critical U.S. diplomatic and information sharing relationships.[98] According to the *National Security Strategy*, the "strategic partnerships and unique relationships we maintain with Canada and Mexico are critical to U.S. national security and have a direct effect on the security of our homeland."[99]

*Pakistan.* The U.S. relationship with Pakistan has been "tragic and tormented."[100] The country's internal instability, complex tribal dynamics, and political ideology have threatened U.S. security and international peace. Pakistan's rapidly growing population, "nuclear arsenal, and relationships with China and India will continue to force it onto the United States' geostrategic map in new and important ways over the coming decades."[101] With respect to diplomatic relations with the U.S., Islamabad is primarily concerned with Afghanistan and the consequences of the rapidly shrinking U.S. military presence.[102]

The Obama Administration claims that Al Qa'ida's remains centered in Pakistan and that this core "remains the most dangerous component of the larger network…."[103] Threats to U.S. national security will increase if the country's governance and security regress to historical levels, if the Taliban maintains control of sections of Afghanistan, and al-Qa'ida is not

---

[95] Peter Grier, "Are Edward Snowden NSA leaks messing up US foreign relations," Christian Science Monitor September 3, 2013 available at http://www.csmonitor.com/USA/DC-Decoder/Decoder-Wire/2013/0903/Are-Edward-Snowden-NSA-leaks-messing-up-US-foreign-relations.

[96] Kathleen Hennessey and Vincent Bevins, "Brazil postpones state visit to U.S. over Snowden spying leaks," LA Times *September 17, 2013, available at* http://www.latimes.com/world/worldnow/la-fg-wn-ff-brazil-us-edward-snowden-spying-leaks-20130917,0,5186201.story#axzz2jmpqWim6.

[97] Richard Chirgwin," Brazil whacks PRISM with secure email plan," The Register, October 14, 2013 available at http://www.theregister.co.uk/2013/10/14/brazil_waxes_lyrical_on_security/

[98] Peter Grier, "Are Edward Snowden NSA leaks messing up US foreign relations," Christian Science Monitor September 3, 2013 available at http://www.csmonitor.com/USA/DC-Decoder/Decoder-Wire/2013/0903/Are-Edward-Snowden-NSA-leaks-messing-up-US-foreign-relations.

[99] National Security Strategy at 42.

[100] Daniel Markey, "No Exit from Pakistan," CFR available at http://www.cfr.org/pakistan/no-exit-pakistan/p31250

[101] Daniel Markey, "No Exit from Pakistan," CFR available at http://www.cfr.org/pakistan/no-exit-pakistan/p31250

[102] See generally WWT at 18.

[103] NSS at 20.

neutralized. According to the *National Security Strategy*, "To prevent future attacks on the United States, our allies, and partners, we must work with others to keep the pressure on al-Qa'ida and increase the security and capacity of our partners in [Afghanistan and Pakistan]."[104]

Beyond the Al Qa'ida threat, the Director of National Intelligence is concerned about the future economic issues in Pakistan. With a very limited tax base, poor tax collection system, and reliance on U.S. foreign aid, the country has no promise of economic growth. These economic circumstances can encourage corruption and the acceptance of terrorist groups who provide much needed currency.[105]

It is undeniably wise to collect intelligence in regions from which these types of national security threats can originate. According to the *Washington Post*, there are intelligence gaps concerning the security of Pakistan's nuclear program, chemical and biological weapons capabilities, and the "loyalties of counterterrorism sources recruited by the CIA."[106] These concerns are so pervasive budget documents are reported to divide the world into two illicit weapons categories: Pakistan and everybody else.[107]

An illegally disclosed summary of the U.S. intelligence community's budget allegedly indicates a significant increase in intelligence activities against Pakistan. This increase may indicate a substantial level of distrust of Pakistan. "They also reveal a more expansive effort to gather intelligence on Pakistan than U.S. officials have disclosed."[108] This belief is supported by Husain Haqqan a former Pakistani ambassador to the United States: "If the Americans are expanding their surveillance capabilities, it can only mean one thing. The mistrust now exceeds the trust."[109] The loss of trust can complicate cooperation with Pakistan intelligence services, restrict intelligence sharing between the two countries, and thus reduce the security of both the U.S. and Pakistan.

The Snowden disclosures are undermining an already tense relationship between the U.S. and Pakistan. The illegal disclosures will likely reduce intelligence sharing and military cooperation at time when threats for both countries are still existential. The disclosures have diminished U.S.

---

[104] NSS at 20

[105] WWT at 18

[106] Greg Miller, Craig Whitlock and Barton Gellman, "Top-secret U.S. intelligence files show new levels of distrust of Pakistan," The Washington Post, September 2 available at http://www.washingtonpost.com/world/national-security/top-secret-us-intelligence-files-show-new-levels-of-distrust-of-pakistan/2013/09/02/e19d03c2-11bf-11e3-b630-36617ca6640f_print.html

[107] Greg Miller, Craig Whitlock and Barton Gellman, "Top-secret U.S. intelligence files show new levels of distrust of Pakistan," The Washington Post, September 2 available at http://www.washingtonpost.com/world/national-security/top-secret-us-intelligence-files-show-new-levels-of-distrust-of-pakistan/2013/09/02/e19d03c2-11bf-11e3-b630-36617ca6640f_print.html

[108] Greg Miller, Craig Whitlock and Barton Gellman, "Top-secret U.S. intelligence files show new levels of distrust of Pakistan," The Washington Post, September 2 available at http://www.washingtonpost.com/world/national-security/top-secret-us-intelligence-files-show-new-levels-of-distrust-of-pakistan/2013/09/02/e19d03c2-11bf-11e3-b630-36617ca6640f_print.html

[109] Greg Miller, Craig Whitlock and Barton Gellman, "Top-secret U.S. intelligence files show new levels of distrust of Pakistan," The Washington Post, September 2 available at http://www.washingtonpost.com/world/national-security/top-secret-us-intelligence-files-show-new-levels-of-distrust-of-pakistan/2013/09/02/e19d03c2-11bf-11e3-b630-36617ca6640f_print.html.

national security by damaging the diplomatic and intelligence relationship with a key ally in a region from whence one of the greatest attacks against the U.S. originated.

The diplomatic and intelligence relationships established over the past sixty years have been critical to the security of the United States. National security is proportionally linked to cooperation with other nations. The quantity and quality of intelligence sharing with foreign intelligence services can reduce the burden and expense on U.S intelligence agencies. Regardless of the veracity of the information illegally disclosed by Snowden, the tensions it is causing within foreign relations must negatively impact the intelligence sharing and cooperation. Less sharing and cooperation equals reduced national security for the U.S.

Intelligence relationships with foreign security services support good partnerships between the U.S. and the partner nation. These relationships provide access to areas the U.S. may not have direct admission. Partners can offer intelligence agility with an ability to collect information that may take longer in the U.S. They provide local insight to a particular target of areas with expertise not resident in the U.S. intelligence community. And relationships with foreign intelligence services may provide cover for U.S. interests by masking American action under their domestic security or military organizations.[110] These advantages have been placed at risk by the recent disclosures of potentially classified information.

**Commercial**

Diplomatic and intelligence cooperation between nations is vital to U.S. national security, but so too is the cooperation between the private and public sectors within the United States. Policy and technology developments over the past sixty years have diminished the capacity of the U.S. government to establish the state-of-the-art technology. This has not always been the case. According to the Intelligence and National Security Alliance:

> Throughout the history of U.S. intelligence, there has been a necessary partnership between government, the private sector, and academia to enhance research, development, manufacturing, and fielding of systems that support the intelligence mission. A broad range of innovations including the earliest computers and dynamic spaceborne collection systems resulted from this partnership.
>
> Through careful attention and nurturing of these partnerships, impressive cutting-edge technologies were developed and utilized on projects including the U-2, SR-71, CORONA overhead collection systems and the CRAY supercomputers.[111]

[110] Rosenbach, Eric and Aki Peritz. "Intelligence and International Cooperation." Memorandum, "Confrontation or Collaboration? Congress and the Intelligence Community," Belfer Center for Science and International Affairs, Harvard Kennedy School, July 2009 available at http://belfercenter.ksg.harvard.edu/publication/19153/intelligence_and_international_cooperation.html

[111] Intelligence and National Security Alliance, "Critical Issues for Intelligence Acquisition Reform: Industry's Assessment of the Intelligence Community Acquisition Process," 1 (October 2008) available at http://www.insaonline.org/i/p/a/i/d/a/Index.aspx?hkey=d73d5c3e-80a5-492b-9fd5-2f7caab8b8da.

Most major defense contractors claim to support intelligence programs throughout the intelligence community.[112] Because the U.S. national security apparatus apparently depends so heavily on the private sector, any damage to that relationship will have a corresponding negative impact on national security. It appears as if the illegal disclosures by Snowden are diminishing national security by causing a rift between high-tech firms and NSA.

A recent letter sent by six leading technology companies is an example of this rift. On October 31, 2013 Facebook, Google, Apple, Yahoo, Microsoft and AOL urged the White House to "work with Congress in addressing…critical reforms that would provide much needed transparency and help rebuild the trust of Internet users around the world."[113] These companies evidently believe that current surveillance practices require re-examination:"Our companies believe that government surveillance practices should also be reformed to include substantial enhancements to privacy protections and appropriate oversight and accountability mechanisms for those programs."[114]

This call for reform – perhaps motivated more by corporate interests than national security interests – may result in less access to information, less cooperation between the public and private sectors, and more bureaucratic demands on the intelligence community when accessing data that has little or no impact on the privacy of U.S. citizens. As noted by the first Assistance Secretary for Policy at the Department of Homeland Security and former General Counsel at the National Security Agency Steweart Baker, "In the long run, any effective method of ensuring privacy is going to have to focus on using technology in a smart way, not just trying to make government slow and stupid."[115] Companies such as Facebook, Google, Apple, Yahoo, Microsoft and AOL handle so much global data and continue to create new ways with which to connect, it is unwise to undermine any speculative partnership with these and similar private companies. Information sharing is already a challenging enough issue for the public and private sectors.

The same principles described by the 9/11 Commission report concerning information within the government, apply to information sharing between the government and the private sector:

> But the security concerns need to be weighed against the costs. Current security requirements nurture overclassification and excessive compartmentalization of information among agencies. Each agency's incentive structure opposes sharing, with risks…but few rewards for sharing information. There are no punishments for not sharing information. Agencies uphold a need-to-know culture of

[112] See generally Booz Allen Hamilton, http://www.boozallen.com/consulting/view-our-work; Northrop Grumma, http://www.northropgrumman.com/capabilities/Pages/default.aspx; Lockheed Martin, http://www.lockheedmartin.com/us/what-we-do/emerging.html; General Dynamics, http://www.gd-ais.com/.
[113] Facebook, Google, Apple, Yahoo, Microsoft and AOL, Letter to The Honorables Leahy, Lee, Conyers, Sensebrenner, October 31, 2013 available at http://sensenbrenner.house.gov/uploadedfiles/usa_freedom_act_letter_10-31-13.pdf.
[114] Facebook, Google, Apple, Yahoo, Microsoft and AOL, Letter to The Honorables Leahy, Lee, Conyers, Sensebrenner, October 31, 2013 available at http://sensenbrenner.house.gov/uploadedfiles/usa_freedom_act_letter_10-31-13.pdf.
[115] Stewart Baker, *Skating on Stilts: Why we aren't stopping tomorrow's terrorism* 314 (2010). Baker's book has enlightened commentary on the privacy issue

> information protection rather than promoting a need-to-share culture of integration.[116]

The current version of the ideas described more than 10 years ago could be that data available to corporations is overly protected and excessively compartmented within the private sector. Each company and government agency should incentivize sharing when national security is at risk. There should be liability for not providing information, rather than liability protections for sharing information with the U.S. government. Both public and private sectors must adopt a culture of integration.

The most recent and likely legislation promoting insufficient, but improved information sharing was S. 2105, The Cybersecurity Act of 2012. This bill – like many other before it – failed to become law because of mutual mistrust between the government and private sector and a suspicion of mutual incompetence.[117] Enhanced information sharing, whether under S. 2105 or any other bill, would have contributed to national security. Because of the disclosures by Snowden, there is now no appetite in Washington to pursue any information exchange between the national security apparatus and corporate America.

According to the *Washington Post*, "The tone of industry reaction to the NSA revelations has grown more aggressive since the first stories appeared in *The Washington Post* and Britain's *Guardian* newspaper in June. Companies that initially were focused on defending their reputations gradually began criticizing the government and challenging it in court. Some companies also have worked to harden their networks against infiltration. A turning point came with the *Washington Post* revealed an NSA program that collects user information from Google and Yahoo as it moves among data centers overseas. To some, this amounted to a degree of intrusiveness that, though speculated about by privacy activists, was beyond what many in the industry thought possible."[118]

The national security impact is clear: less cooperation between the U.S. national security departments and agencies will result in less or more difficult access to data and less or more difficult access to technical innovation.

**Public Confidence**

The American National Security Strategy "begins with a commitment to build a stronger foundation for American leadership, because what takes place within our borders will determine our strength and influence beyond them."[119] What is taking place within our borders in response to the disclosures of potentially classified information is reducing U.S. national security by undermining public confidence in the National Security Agency, the Intelligence Community,

---

[116] 9/11 Commission Report at 417.

[117] See generally, Charles Abbott, "Cybersecurity bill dead after second U.S. Senate rebuff," Reuters Nov 14, 2012, available at http://www.reuters.com/article/2012/11/15/us-usa-cyber-legislation-idUSBRE8AE04720121115.

[118] Craig Timberg and Ellen Nakashima, "Amid NSA spying revelations, tech leaders call for new restraints on agency," (October 31, 2013) available at http://www.washingtonpost.com/world/national-security/amid-nsa-spying-revelations-tech-leaders-call-for-new-restraints-on-agency/2013/10/31/7f280aec-4258-11e3-a751-f032898f2dbc_print.html.

[119] NSS at 2.

and the federal government. The daily media indictments of one of the premier intelligence agencies in history is disrespectful to the thousands of American citizens who work at NSA, and has presented the public with an inaccurate image of intelligence community oversight. The loss of public trust resulting from amateur media analysis and by Snowden's actions is already damaging national security by distracting national security professionals from their jobs. In our democracy, reductions in public support and agency credibility will inevitably result in fewer resources, reduced authority, and additional scrutiny. For students of national security history, this portends a pendulum swing back to less information sharing, less authority to collect intelligence vital to U.S. national security, and a reversion to less sharing of information within the U.S. government and with foreign allies.

According to a Pew Research poll conducted shortly after the first illegal disclosures by *the Guardian*, "for the first time since 9/11, Americans are now more worried about civil liberties abuses than terrorism."[120] According to Pew, 56 percent of Americans believe U.S. federal courts have inadequately limited counter-terrorism telephone and internet data collection by the government. "An even larger percentage (70%) believes that the government uses this data for purposes other than investigating terrorism."[121] This data show the misunderstanding of the value of the alleged NSA programs, despite congressional testimony and declassified documents that demonstrate that these programs have stopped violent attacks against the U.S. and its allies. Regardless of the value of the disclosed activities, the political reaction has been swift.

President Obama announced in early August that reforms were coming for NSA surveillance. Section 215 of the USA Patriot Act and the role of the Foreign Intelligence Surveillance Court are now under review. "Obama wants to let a civil liberties representative weigh in on the court's deliberations to ensure that an adversarial voice is heard and will form a high-level group of outside experts to review the U.S. surveillance effort."[122] The president has also ordered the declassification of many documents surrounding the collection of data in the hope of restoring the public trust damaged by the recent disclosures.

Congress has also announced its own reforms. The Intelligence Oversight and Surveillance Reform Act[123], introduced by Senators Ron Wyden, Mark Udall, Richard Blumenthal, and Rand Paul, will "prohibit bulk collection of Americans' records, shield Americans from warrantless searches of their communications and install a constitutional advocate to argue significant cases before the secret Foreign Intelligence Surveillance court."[124] No action has been taken on the bill since its introduction on September 25, 2013.

---

[120] Glenn Greenwald, "Major opinion shifts, in the US and Congress, on NSA surveillance and privacy," The Guardian July 26, 2013 available at http://www.theguardian.com/commentisfree/2013/jul/29/poll-nsa-surveillance-privacy-pew.

[121] Pew Research Center for People and the Press, "Few See Adequate Limits on NSA Surveillance Program," July 26, 2013 available at http://www.people-press.org/2013/07/26/few-see-adequate-limits-on-nsa-surveillance-program/.

[122] Steve Holland And Jeff Mason," Obama says reform ahead for NSA surveillance program," Milwaukee Wisconsin Journal Sentinel, August 9, 2013 available at http://www.jsonline.com/news/usandworld/obama-begins-news-conference-addresses-nsa-b9972397z1-219024921.html

[123] S. 1551 available at https://www.govtrack.us/congress/bills/113/s1551/text

[124] Senator Ron Wyden, "Surveillance Reform Package Ends Bulk Collection of Phone Records; Creates Constitutional Advocate for Secret Court," Press Release, September 25, 2013 available at

Congress has also considered an amendment to the Defense Appropriations bill that would restrict NSA's access to data.[125] It was the first legislative challenge to programs that the White House, the Office of the Director of National Intelligence, the Department of Justice, and the National Security Agency have claimed have stopped violent attacks against the U.S. The amendment was defeated by 12 votes in the House of Representatives sending a clear message to the Obama Administration that there is anxiety about the program. "Though the amendment barely failed, the vote signaled a clear message to the NSA: we do not trust you."[126]

The Snowden disclosures may also have larger implications for other elements of the U.S. government. As a consequence of the disclosures, Congress and the executive branch are considering placing a political appointee at the head of the National Security Agency and separating the roles of Director, NSA and Commander, U.S. Cyber Command. According to the *Washington Post*, "National Security Council officials are scheduled to meet soon to discuss the issue of separating the leadership of the National Security Agency and Cyber Command, a shift that some officials say would help avoid an undue concentration of power in one individual and separate entities with two fundamentally different missions: spying and conducting military attacks. The administration is also discussing whether the NSA should be led by a civilian."[127]

With the reduction in potential legal authority for NSA, public sentiments against the NSA surveillance that has contributed so much to national security and the pressures that are a consistent feature of budget negotiations, can reductions to the NSA budget be far behind? With less money, less authority, and less credibility, NSA will wind up with fewer people, less data, and impoverished contributions to national security. According to top agency counsels, reforms under consideration may reduce Americans privacy in an effort to enhance it. Lawyers from the Intelligence Community are now arguing against certain reforms, in support of the status quo.[128]

Perhaps it was inevitable that the national security apparatus constructed since 9/11 would be dismantled when Americans no longer view the threat to the U.S. as starkly as they did on September 11, 2001. With political dysfunction, government shutdown, unemployment, perhaps al-Qaeda, Iran's nuclear program, Muslim extremism, and nuclear proliferation are no longer worth allowing the NSA to access metadata.

---

http://www.wyden.senate.gov/news/press-releases/surveillance-reform-package-ends-bulk-collection-of-phone- records-creates-constitutional-advocate-for-secret-court

[125] See generally, Justin Amash, Amash NSA Amendment Fact Sheet July 24, 2013 available at http://amash.house.gov/speech/amash-nsa-amendment-fact-sheet

[126] http://www.theguardian.com/commentisfree/2013/oct/25/nsa-no-congress-oversight

[127] Ellen Nakashima, "U.S. weighs option to end dual leadership role at NSA, Cyber Command," Washington Post November 6, 2013 available at http://www.washingtonpost.com/world/national-security/us-weighs-proposal-to-end-dual-leadership-role-at-nsa-cyber-command/2013/11/06/e64a23d8-4701-11e3-b6f8-3782ff6cb769_story.html.

[128] John Hudson, "Top Obama Lawyers: Reforming the NSA Could Hurt Americans' Privacy," Foreign Policy blog November 4, 2013 available at http://thecable.foreignpolicy.com/posts/2013/11/04/top_obama_lawyers_reforming_the_nsa_could_hurt_americans_privacy_rights.

As noted by lawyer, diplomat, writer, and philosopher Joseph de Maistre, "Every nation gets the government it deserves."[129] If the citizens of the American republic demand a reduction in their own security as a result of actions taken in violation of laws their representatives established, then we will not only get the government we deserve, but also the level of security we have chosen.

**Conclusion**

Regardless of the legitimacy, or lack thereof, of Snowden's actions, the material he has revealed in violation of law, regulation, and oath has placed U.S. security at risk. The disclosures have resulted in significant damage to diplomatic relationships with countries that share intelligence with the U.S., domestic commercial relationships between the U.S. public and private sectors leading to less information sharing and innovation, and damage to the public confidence in the NSA leading to fewer resources and authority to protect the U.S. in the manner that it has done so since 9/11. The disclosures will also facilitate operational changes in the behavior of current adversaries' practices and attention to the protection of their information; the damage to It will become more difficult, more expensive, and more time consuming to collect and analyze information on terrorist groups, foreign governments, and foreign militaries.

Our Republic is resilient and will survive the exposure of the "plumbing" of NSA's intelligence apparatus.[130] Surviving will be more dangerous, more expensive, and take more time than reforms would have required absent Snowden's illegal activities. Just as Snowden must do on his own, we must all ask ourselves if the transparency that he has forced onto the system is worth the diminishing of American security.

[129] Bartlett's Roget's Thesaurus, 2003,

[130] See generally comments from Michael V. Hayden during the Washington Post Live's Cyber Summit, 3 October 2013 avaiable at http://www.washingtonpost.com/postlive/conferences/cybersecurity-2013

Preliminary Draft – Please Do Not Cite Without Permission
To be Published in *I/S: A Journal of Law and Policy for the Information Society*
9 ISJLP ___ (2014).
http://www.is-journal.org

# *National Insecurity: The Impacts of Illegal Disclosures of Classified Information*

Mark D. Young*

> There had never been anything like it. In today's terms, it was as if an NSA employee had publicly revealed the complete communications intelligence operations of the Agency for the past twelve years-all its techniques and major successes, its organizational structure and budget-and had, for good measure, included actual intercepts, decrypts, and translations of the communications not only of our adversaries but of our allies as well.[1]

In the mid-summer of 2013, the British newspaper, *The Guardian*, published claims by a contractor for the National Security Agency (NSA) that millions of telephone records were being collected under an order from the Foreign Intelligence Surveillance Court. Throughout the summer, additional disclosures about apparent surveillance operations seized headlines around the world. Interpreting the meaning of the disclosures has been more complicated, but it is clear that there is great interest in United States intelligence activities.

Despite being fired from his contractor position with Booz Allen Hamilton[2] and charged with espionage and theft, Edward Snowden continued to provide classified information to *The Guardian*. The paper has published more than 300 stories on signals intelligence methodologies, the statutes and court authorities under which the United States Intelligence Community conducts these operations, and the intelligence relationships between foreign governments and the United States.[3]

These disclosures of sensitive and classified information concern not only the United States, but also its allies. The material disclosed by Snowden has implicated the United Kingdom's Government Communications Head Quarters (GCHQ). British government concerns about the potential publication of classified data were significant enough to threaten *The Guardian* with legal action if the information was not destroyed. The threats prompted the destruction of hard drives containing information related to GCHQ.[4]

---

*Mark D. Young is the President and General Counsel of Ronin Analytics, LLC. Previously he served as the Executive Director for the Directorate of Plans and Policy at United States Cyber Command, the Special Counsel for Defense Intelligence for the House Permanent Select Committee on Intelligence, and as a senior leader at the National Security Agency. The views expressed in this article are those of the author and do not reflect the official policy or position of the U.S. government. This article is derived entirely from open source material and contains no classified information.

[1] National Security Agency, "The Many Lives of Herbert O. Yardley," *Crytptologic Spectrum* (Autumn 1981, 12) at

10.

[2] http://articles.latimes.com/2013/jun/11/news/la-pn-edward-snowden-fired-booz-allen-20130611

[3] http://www.theguardian.com/world/2013/aug/21/edward-snowden-nsa-files-revelations

[4] Julian Borger, "NSA files: why the Guardian in London destroyed hard drives of leaked files," The Guardian August 20, 2013 available at http://www.theguardian.com/world/2013/aug/20/nsa-snowden-files-drives-destroyed-

The national security implications of the disclosure of this information are significant. According to the most experienced U.S. intelligence officer, Michael V. Hayden,[5] "Edward Snowden will likely prove to be the most costly leaker of America secrets in the history of the Republic."[6] The Chairman of the House Intelligence Committee has noted that Snowden has jeopardized U.S. national Security" by exposing on-going U.S. counterterrorism activities.[7] The Director of National Intelligence stated, "The unauthorized disclosure of a top secret U.S. court document threatens potentially long-lasting and irreversible harm to our ability to identify and respond to the many threats facing our nation."[8]

Snowden claims that his disclosures – in violation of law, regulation, and his solemn oath – are motivated by his judgment about the value of the intelligence. He removed and released data that allegedly shows how the National Security Agency had collected information on civilian institutions, to include universities, hospitals, and businesses. Snowden claims these alleged NSA operations are dangerous and criminal: "These nakedly, aggressively criminal acts are wrong no matter the target."[9] Without referencing the multiple layers of intelligence oversight within the Department of Defense, the Office of the Director of National Intelligence, the National Security Agency's Inspector General, and the Intelligence Community Inspector General, Snowden concluded that "the public needs to know the kinds of things a government does in its name, or the "consent of the governed" is meaningless."[10]

Regardless of one's sympathy for Snowden's conclusion, the scope and scale of the material he has revealed will continue to have a significant impact on United States national security. There are four areas where his actions will diminish national security. First, the disclosure of the programs, relationships, and operations will facilitate operational changes in the behavior of adversarial groups such as al-Qaida and Hamas.[11]It will become more difficult, more expensive, and more time consuming to collect and analyze information on terrorist groups, foreign governments, and foreign militaries.

Second, the disclosures will complicate U.S. foreign relations that directly contribute to U.S. security interests. Cooperation between U.S. and foreign intelligence organizations is critical to the security of the U.S.[12] Other countries are perpetually concerned about disclosing sensitive

---

london. This destruction has not prevented the further disclosures of classified data, however, since the reporter who first broke the story, had additional copies of the material in Brazil and in the United States (http://www.theguardian.com/world/2013/aug/20/nsa-david-miranda-guardian-hard-drives).

[5] General Michael V. Hayden is a career military intelligence officer who led the Central Intelligence Agency, the National Security Agency, and was the first Principal Deputy Director of National Intelligence.

[6] http://www.cnn.com/2013/07/19/opinion/hayden-snowden-impact/index.html

[7] Rogers Video, http://www.mediaite.com/tv/gop-rep-rogers-blasts-snowden-just-go-to-north-korea-iran-to-round-out-government-oppression-tour/

[8] ODNI, DNI Statement on Recent Unauthorized Disclosures of Classified Information June 6, 2013

[9] Edward Snowden: NSA whistleblower answers reader questions, http://www.theguardian.com/world/2013/jun/17/edward-snowden-nsa-files-whistleblower

[10] Edward Snowden: NSA whistleblower answers reader questions, http://www.theguardian.com/world/2013/jun/17/edward-snowden-nsa-files-whistleblower

[11] See generally "Country reports on terrorism". U.S. State Dept. May 27, 2005. Archived from the original on May 11, 2005. Retrieved 2008-01.26.

[12] The National Strategy for Information Sharing and Safeguarding (December 2012) highlights the importance of sharing with partner nations, "our national security depends upon an ability to make information easily accessible to

information collected by their intelligence services at great expense and effort. Snowden has now exacerbated these concerns and weakened traditionally strong American assurances that information provided to the U.S. will be well protected with little risk of embarrassment or compromise to the providing country. It will become more difficult to cooperate with these partners when there is a stream of evidence that shows that the United States cannot keep a secret.

Third, Snowden's actions have impaired cooperation between the United States government and the U.S. private sector. It was already challenging to share information between the U.S. public and private sectors[13], but the exposure of alleged relationships – whether voluntary or pursuant to a court order - between companies such as Verizon, Google, and Facebook has made corporate entities recoil from the government in fear of a diminished reputation or decline in stock value.

Finally, despite Snowden's claimed objective of exposing an "architecture of oppression"[14] his violation of law, regulation, and oath has eroded the confidence of the American public he was hoping to inform. In our representative democracy, this loss of public confidence will quickly transform into fewer resources for the very departments and agencies that safeguard America. Less authority and more oversight are sure to follow. It is understandable, but the reduction in funding, authority and the increase in oversight are the type of emotionally satisfying reactions that will undermine U.S. national security.

These four consequences of Snowden's illegal exposures of classified data will diminish U.S. national security particularly in the short term. It is possible that the reforms and examination of technical collection and analysis will become stronger in the long term, but this is unlikely in the context of rapidly diminishing government funding, continuing economic hardships, and in an environment in which national security may not be in the forefront of the minds of U.S. citizens.

The current administration's National Security Strategy, published in May 2010 provides the focus for an examination of the impacts of the Snowden disclosures.[15] This strategy prioritizes American leadership by "shaping an international order that can meet the challenges of our time" and "recognizes the fundamental connection between our national security, our national competitiveness, resilience, and moral example."[16] U.S. national security interests are: Strengthening Security and Resilience at Home, the Disruption, Dismantling, and Defeat of Al-Qa'ida and its Violent Extremist Affiliates, the Use of Force only as a last resort, the Reverse the Spread of Nuclear and Biological Weapons, the Advancement of Peace, Security, and Opportunity in the Greater Middle East, the Investment in the Capacity of Strong and Capable Partners, and the Securing of Cyberspace.

---

Federal, state, local, tribal, territorial, private sector, and foreign partners in a trusted manner, given the appropriate mission context." Page 7

[13] See generally, Jennifer Martinez and Ramsey Cox "Senate votes down Lieberman, Collins Cybersecurity Act a second time," The Hill November 14, 2012 available at http://thehill.com/blogs/hillicon-valley/technology/268053-senate-rejects-cybersecurity-act-for-second-time.

[14] Video, First Interview at around 7:00, http://www.theguardian.com/world/video/2013/jun/09/nsa-whistleblower-edward-snowden-interview-video

[15] National Security Strategy (2010), available at http://www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf

[16] NSS at 1.

Consistent with the U.S. national security interests are the global and regional threats outlined by the Director of National Intelligence in April 2013. The Increasing Risk to US Critical Infrastructure, Eroding US Economic and National Security, and Information Control and Internet Governance put cybersecurity at the top of the DNI's Worldwide Threat Assessment.[17] Terrorism and Transnational Organized Crime, and the proliferation of weapons of mass destruction were also listed as global threats. With respect to regional threats, Middle East and North Africa (Egypt, Syria, Iran, Iraq, Yemen, Lebanon, and Libya) were listed as threats because the transitioning governments within this region are at risk of failing to "address public demands for change" and "are likely to revive unrest and heighten the appeal of authoritarian or extremist solutions."[18] The information disclosed by Snowden is negatively affecting the national security community's ability to collect and analyze information concerning each of these regional and transnational threats.

**Operational Shifts**

> "Discussing programs like this publicly will have an impact on the behavior of our adversaries and make it more difficult for us to understand their intentions."[19]

The classified material published by the Guardian and other media describes in significant detail the methodologies apparently employed by the National Security Agency in the conduct of its mission. Established in 1952, NSA produces signals intelligence[20] and protects U.S. communications from interception. According to David Kahn, "In intelligence, [NSA] intercepts, traffic-analyzes, and cryptoanalyzes the messages of other nations, friend as well as foe."[21] In addition, NSA executes "the responsibilities of the Secretary of Defense as executive agent for the communications security of the United States Government."[22] This means that the Agency must provide technical and practical means to ensure that no other parties can benefit from the collection of U.S. communications.

Examples of NSA's contributions to national security are difficult to find because of the sensitivity of the Agency's mission. In recent congressional testimony, however, the Director of National Intelligence said that SIGINT is the primary contributor to counterterrorism intelligence and that multiple empirical studies have shown that signal intelligence, provided by NSA, is the major contributor to answering the hardest intelligence challenges faced by the United States.[23]

---

[17] James R. Clapper, Director of National Intelligence, Worldwide Threat Assessment of the US Intelligence Community Statement for the Record before the House Permanent Select Committee on Intelligence (April 11, 2013) 3 available at http://www.dni.gov/files/documents/Intelligence%20Reports/2013%20WWTA%20US%20IC%20SFR%20%20HPSCI%2011%20Apr%202013.pdf.

[18] Worldwide Threat Assessment at 14.

[19] ODNI DNI Statement on recent …

[20] Intelligence comprising communications intelligence, electronic intelligence, and foreign instrumentation signals intelligence.

[21] David Kahn, The Code Breakers: The Comprehensive History of Secret Communication from Ancient Times to the Internet 675 (Second edition, 1996)

[22] Exec. Order No. 12,333, as amended.

[23] USHR19 Joint Committee on Homeland Security , October 29 questioning by Rep. Thornberry to DNI Clapper at 4:36 available at http://www.ustream.tv/recorded/40304984.

Although the claims in the books are unconfirmed, publications such as *Counter Strike: The Untold Story of America's Secret Campaign Against Al Qaeda* by Eric Schmitt and Thom Shanker and *Operation Dark Heart; Spycraft and Special Ops on the Frontlines of Afghanistan – and the Path to Victory* by Lieutenant Colonel Anthony Shaffer suggest that NSA may have prevented significant terrorist attacks and provided critical intelligence during U.S. military operations.

These books, together with the claims of senior intelligence officials before Congress, strongly suggest that NSA's efforts are the most effective shield against the acts of violence to harm Americans and our national security interests. In response to apparent disclosures of NSA activities, President Obama directed the declassification of sensitive NSA collection conducted under the Foreign Intelligence Surveillance Act (FISA). In September 2013, multiple documents concerning "bulk telephony metadata" collection under Section 501 of FISA were declassified and publically released by the Office of the Director of National Intelligence.[24] These disclosures included a Foreign Intelligence Surveillance Court finding of reasonable grounds that the call records were relevant to an authorized terrorism investigation.[25] The same order required NSA to establish "mandatory procedures strictly to control access to and use of the archived data collected pursuant to [the court's] order." Additionally, the order mandated that NSA's General Counsel monitor the designation of those with access to the data and act as an approval authority for the actual queries analysts wished to make of the data.[26]

In late October 2013, the ODNI released a number of additional documents related to NSA's alleged collection programs. These documents include a 2009 congressional notification describing the failure to comply with a Foreign Intelligence Surveillance Court order,[27] and a March 2009 Internal NSA Memorandum of Understanding required for access and query privileges of data collected through NSA's bulk telephony metadata program.[28] These documents describe the legal justifications for and technical detail about how the National Security Agency collects and uses intelligence.

---

[24] Office of the Director of National Intelligence, DNI Clapper Declassifies Additional Intelligence Community Documents Regarding Collection Under Section 501 of the Foreign Intelligence Surveillance Act (October 28, 2013) available at http://www.dni.gov/index.php/newsroom/press-releases/191-press-releases-2013/954-dni-clapper-declassifies-additional-intelligence-community-documents-regarding-collection-under-section-501-of-the-foreign-intelligence-surveillance-act. FISA Section 501 was amended by Section 215 of the USA PATRIOT Act (Section 215) in 2001. P.L. 107-56?

[25] FISA Ct., Order In Re Application of the Federal Bureau of Investigation for An Order Requiring The Production of Tangible Things From____, at 3 Docket No. BR 06-05 available at http://www.dni.gov/files/documents/section/pub_May%2024%202006%20Order%20from%20FISC.pdf

[26] FISA Ct., Order In Re Application of the Federal Bureau of Investigation for An Order Requiring The Production of Tangible Things From____, at 5-6 Docket No. BR 06-05 available at http://www.dni.gov/files/documents/section/pub_May%2024%202006%20Order%20from%20FISC.pdf

[27] National Security Agency, Memorandum for the Staff Director, House Permanent Select Committee on Intelligence, Congressional Notification: Incidents of Noncompliance – Information memorandum (February 25, 2009) available at http://www.dni.gov/files/documents/501/25%20Feb%2009%20NSA%20CN_SealedFINAL.pdf.

[28] Available at http://www.dni.gov/files/documents/501/Mem%20of%20Understanding%20for%20H2I4%20HMCs_Sealed%20FINAL.pdf

This information was declassified and publically released to inform the public about what data were collected and analyze by NSA, to balance inaccurate speculations by the media about NSA, and to facilitate the debate about U.S. intelligence Community operations. When examined together, the information disclosed by Snowden and the declassified information released by the ODNI present a positive picture of prudent measures for national security. If the information about programs such as PRISM, FAIRVIEW, or OAKSTAR is accurate, then it appears as if the intelligence community has not only adjusted well to global technical advancements in telecommunications, but also learned significant lessons from the September 11, 2001 terrorist attacks.

It was known in early 2001 that NSA's effectiveness was challenged by the "multiplicity of new types of communications links, by the widespread availability of low-cost encryption systems, and by changes in the international environment in which dangerous security threats can come from small, but well organized, terrorist groups as well as hostile nation states."[29] Any challenge about the value of an intelligence program must address the importance of data quantity and quality. First, since intelligence analysis depends on having access to relevant information, logic dictates that more data is always better. As noted by Mark Lowenthal:

> The issue then becomes how to extract the intelligence from the mountain of information. One answer would be to increase the number of analysts who deal with the incoming intelligence, but that raises further demands on the budget. Another possible response, even less palatable, would be to collect less. But, even then, there would be no assurance that the "wheat" remained in the smaller volume still being collected.[30]

Thus, quantity has an intelligence quality all its own. In addition, the type of information needed by the intelligence community is also important. Given the priorities noted in the National Security Strategy, the importance of NSA collection and analysis as noted in congressional testimony and the ever-present threats by terrorist groups and hostile nations the American public should vigorously endorse the type of programs viewed by Snowden as oppressive. It is troubling to see the disclosure of techniques allegedly used by NSA to obtain "cryptographic details of commercial cryptographic information security systems through industry relationships,"[31] and the rampant speculation about the monitoring of the mobile phones of the heads of state from Europe.

It is not only logic that leads one to believe in the value of NSA collection, but also testimony by intelligence professionals. For example, according to the House Intelligence Committee, NSA activities have "been integral in preventing multiple terrorist attacks, including a plot to attack on the New York Stock Exchange in 2009."[32] The PRISM program – a program reported to provide

---

[29] Richard A. Best, Jr., *The National Security Agency: Issues for Congress* 1 Congressional Research Service January 16, 2001 available at http://www.fas.org/irp/crs/RL30740.pdf.
[30] Mark M. Lowenthal, *Intelligence: From Secrets to Policy* 55 (2000).
[31] theguardian.com, "NSA: classification guide for cryptanalysis" 5 September 2013 available at http://www.theguardian.com/world/interactive/2013/sep/05/nsa-classification-guide-cryptanalysis
[32] HPSCI Urge of support for NSA, http://intelligence.house.gov/press-release/chairman-mike-rogers-and-ranking-member-dutch-ruppersberger-urge-support-important-nsa.

NSA access to information some of the largest technology companies - provided "critical leads" to disrupt more than 50 potential terrorist events in more than 20 countries. The Foreign Intelligence surveillance Act authority - the congressional authorization to target communications of foreign persons who are located abroad for foreign intelligence purposes - contributed to more than 90 percent of these disruptions.[33]

The Deputy Attorney General has noted that the Federal Bureau of Investigation benefited from NSA's Section 702 collection in the fall of 2009. Using Section 702 collection and "while monitoring the activities of Al Qaeda terrorists in Pakistan, the National Security Agency (NSA) noted contact from an individual in the U.S. that the Federal Bureau of Investigation (FBI) subsequently identified as Colorado-based Najibulla Zazi. The U.S. Intelligence Community, including the FBI and NSA, worked in concert to determine his relationship with Al Qaeda, as well as identify any foreign or domestic terrorist links."[34]

"The FBI tracked Zazi as he traveled to New York to meet with co-conspirators, where they were planning to conduct a terrorist attack. Zazi and his co-conspirators were subsequently arrested. Zazi, upon indictment, pled guilty to conspiring to bomb the NYC subway system. Compelled collection (authorized under Foreign Intelligence Surveillance Act, FISA, Section 702) against foreign terrorists was critical to the discovery and disruption of this threat against the U.S."[35] Regardless of the accuracy of the information released by Snowden, the types of programs described by the material contribute to national security and its released, regardless of its validity will negatively impact US security.

Homegrown Violent Extremists[36] continue to be inspired by global jihadist propaganda and the perceived success of plots such as the November 2009 attack at Fort Hood, Texas and the March 2012 attacks by an al-Qa'ida-inspired extremist in Toulouse, France.[37] The threat from terror groups remains existential and of great concern to the U.S. intelligence community. The revelations concerning the NSA's counterterrorism successes will motivate terror groups to reexamine how they communicate, plan, and execute these attacks.

*Terror Groups*. It is likely t hat terrorist groups will change how they conceive, plan, and execute terrorist attacks as a result of the classified intelligence information now exposed to the public. Terrorist groups continuously adjust their methodologies for attacking their targets[38], but the recent disclosures provide a roadmap for terror groups to avoid detection.

---

[33] HPSCI Open hearing around 37:30 http://www.c-spanvideo.org/program/AgencyOp

[34] HPSCI Web page, http://intelligence.house.gov/1-four-declassified-examples-more-50-attacks-20-countries-thwarted-nsa-collection-under-fisa-section and CSPAN HPSCI Hearing at 39:30

[35] HPSCI Web page, http://intelligence.house.gov/1-four-declassified-examples-more-50-attacks-20-countries-thwarted-nsa-collection-under-fisa-section

[36] *See generally* Jerome P. Bjelopera, American Jihadist Terrorism: Combating a Complex Threat 5 Congressional Research Service (R41416 )(January 23, 2013) (Homegrown violent extremists are jihadist-inspired American citizens or legal permanent residents that plan or conduct terrorist attacks on the United States.) available at http://www.fas.org/sgp/crs/terror/R41416.pdf

[37] WWT SFR at 4

[38] According to the Director of National Intelligence, Al-Qa'ida in the Arabian Peninsula remains focused on attacks on US soil and "continues to adjust its tactics, techniques and procedures for targeting the West." (WWT at 3)

As similar example of how terrorist groups adjust their planning and communication techniques in response to the disclosure of classified information is found in the 9/11 Commission report. Referring to a 1998 *Washington Times* story disclosing that Osama Bin Laden communicated with a satellite phone, the 9/11 Commission noted that al Qaeda's senior leadership "had stopped using a particular means of communication almost immediately after a leak to *The Washington Times*. This made it much more difficult for the National Security Agency to intercept his conversations."[39] Despite the controversy surrounding this story, it makes logical sense that terror groups will not use technologies reportedly monitored by those who seek to disrupt their plans.

Similar changes in terror group practices as reported by the *New York Times* can be anticipated with the Snowden disclosures. The details of how intelligence targets will alter their practices are speculative given the obscurity of terrorist methodologies, but a few points are clear.

If the reports are true and NSA can exploit[40] the "worldwide use of nine U.S.-based Internet service providers, including Google, Yahoo, Skype and YouTube," then it is reasonable to assume that terrorist groups using these technologies or services will discontinue use of these services. According to the *New York Times*, the Snowden disclosures resulted in jihadists posting Arabic news articles about [NSA's capabilities] … and recommended fellow jihadists to be very cautious, not to give their real phone number and other such information when registering for a website." [41] Similar posts recommending jihadists use "privacy-protecting email systems like The Onion Router, to hide their computer's IP address, and to use encrypted links to access jihadi forums"[42] provide direct evidence that the recent disclosures will change how terrorists plan and conduct their attacks.

Another example concerns alleged NSA access to Skype. Purchased by Microsoft in 2011, Skype claims to employ standard encryption to protect users from hackers and criminals.[43] Documents published by the Guardian suggest that NSA may have had access to Skype servers.[44] Despite this suggested access, others claim that Skype calls made to other Skype customers were untraceable because of Skype corporate location. "Skype is located in Luxembourg (outside of the United States), and…[encryption] keys used by Skype cannot be turned over to the FBI because Skype does not hold the keys themselves. The key is only known by the computers using the program to connect with each other, and Internet communication is inherently hard to trace because of how packets can be routed."[45]

---

[39] 9/11 Commission report at 127

[40] Taking full advantage of any information that has come to hand for tactical, operational, or strategic purposes. (JP 1-02 at 96)

[41] http://nypost.com/2013/06/26/terrorists-to-ditch-skype-and-youtube-after-leaks-reveal-nsa-surveillance-tactics/

[42] http://nypost.com/2013/06/26/terrorists-to-ditch-skype-and-youtube-after-leaks-reveal-nsa-surveillance-tactics/

[43] http://www.skype.com/en/security/#encryption (Inaccessible as of 11/17; use https://support.skype.com/en/faq/FA31/does-skype-use-encryption?frompage=search&q=encryption&fromSearchFirstPage=false)

[44] NSA Prism program slides, The Guardian, 1 November 2013 available at http://www.theguardian.com/world/interactive/2013/nov/01/prism-slides-nsa-document

[45] http://www.unitedliberty.org/articles/talk-like-a-terrorist-use-skype (However, see http://www.nytimes.com/2013/09/06/us/nsa-foils-much-internet-encryption.html?hp&pagewanted=all&_r=0).

As early as 2011, reports described how terrorist use of Skype was hindering law enforcement in India. According to the *Times of India*, "Terrorist organizations targeting India have moved their communications significantly to Internet and other possible innovative means, denying Indian intelligence agencies any major breakthrough yet in their post-Mumbai blasts investigations." [46] Kashmiri terrorists are reportedly using smart phones and Skype according to a senior Indian Army officer. Terrorists, like the general population, migrate to technologies that enhance communications. The popularity and proliferation of Skype supports the hypothesis that international terror groups have used Skype.

Regardless of the validity of the reports of NSA access to Skype servers or the inability of access to Skype communications, the new attention to alleged Skype vulnerabilities will encourage illicit users to move to other technologies. By exposing real or imagined capabilities of the U.S. Intelligence Community, potential state and non-state targets of electronic surveillance are better equipped to avoid surveillance by avoiding specific technologies and technical services.

One such service is the Society for Worldwide Interbank Financial Telecommunications (SWIFT) network. SWIFT, a member-owned cooperative, enables the standardized exchange of proprietary financial data such as payments, securities, and bank commodity trades.[47] Financial transactions, such as those facilitated by SWIFT, are a direct concern to counterterrorism officials. The 9/11 Commission noted, "Vigorous efforts to track terrorist financing must remain front and center in U.S. counterterrorism efforts. The government has recognized that information about terrorist money helps us understand their network, search them out, and disrupt their operations."[48]

In support of this understanding, an intergovernmental policymaking group established to address money laundering issues in 1989, expanded its mission to include "identifying sources and methods of terrorist financing and adopted nine special recommendations on terrorist financing to track terrorists' funds."[49] The Financial Action Task Force on Money Laundering, comprised of 36 member countries, was develops and promotes "policies to combat money laundering and terrorist financing."

Because terror financing became a priority well before September 11, 2001 the European Union and U.S. began to permit US agencies "limited access to bank data transferred through the SWIFT network." The agreement supported the US Terrorist Finance Tracking Program established after the September 11 attacks.[50] Recent disclosures have focused attention on the data reportedly accessed by NSA.

---

[46] http://articles.timesofindia.indiatimes.com/2011-07-19/india/29790655_1_satellite-phones-intelligence-agencies-thuraya

[47] See generally SWIFT Company information available at http://www.swift.com/about_swift/company_information/company_information and "FIN traffic "available at http://www.swift.com/assets/swift_com/documents/about_swift/SIF_2013_09.pdf

[48] 9/11 Commission report at 382.

[49] James K. Jackson, The Financial Action Task Force: An Overview at "Summary" May 9, 2012 (CRS)( RS21904) available at http://www.fas.org/sgp/crs/misc/RS21904.pdf

[50] JERIN MATHEW, "Edward Snowden NSA Scandal: EU to Suspend US Data Sharing After Swift's Interbank Messaging System Breach," International Business Times (September 25, 2013) available at http://www.ibtimes.co.uk/articles/508882/20130925/edward-snowden-nsa-scandal-swift-tftp-eu.htm

In response to this arrangement being made public, the European Union has threatened to "suspend or even terminate the crucial EU-US Terrorist Finance Tracking Programme."[51] The national security impact of this disclosure is the potential loss of an apparently valued source of financial intelligence.[52] The importance of terrorist financing is self-evident. If, pursuant to an international agreement, NSA had access to international money transfers, it is reasonable to believe that U.S. intelligence community was well positioned to interdict the planning and execution of violent actions against the U.S. of her allies. If financial transfers are moved as a result of the illicit disclosures of collection of networks such as SWIFT, then U.S. understanding and ability to prevent terrorist actions is significantly degraded.

Snowden's disclosures have already changed terror group's practices making it more difficult for U.S. intelligence agencies to provide warnings about terror groups' plans and intentions. The loss of insight into these targets diminishes U.S. security, but also prevents the U.S. from sharing information with its allies and partners, diminishing U.S. global influence. The net effect of Snowden's disclosures is to increase terrorist consciousness of their own vulnerabilities. Their response has been immediate and may have a dangerous cumulative effect.[53]

**Foreign Relations**

> However the Snowden episode turns out ... what it mainly illustrates is that we are living in an age of American impotence. The Obama administration has decided it wants out from nettlesome foreign entanglements, and now finds itself surprised that it's running out of foreign influence.[54]

Beyond the national security impact of making terrorist intentions and plans harder to discover and the change in practices of terrorist and opposition groups, Snowden's release of classified information will diminish national security by degrading U.S. foreign relations. American security relies heavily on foreign partnerships that have increased in breadth and scope since the September 11, 2001 terrorist attacks.

Foreign governments are likely to share less information and require more scrutiny of future interactions with U.S. intelligence and no country allegedly targeted for collection is pleased to see the public reports about it. Rising anti-Americanism will strain already tense relationships with countries such as Russia and China; European Union officials have expressed outrage over the Snowden disclosures.[55] The reports have already distracted the U.S. and Russian delegations

---

[51] Jerin Mathew , "Edward Snowden NSA Scandal: EU to Suspend US Data Sharing After Swift's Interbank Messaging System Breach," International Business Times (September 25, 2013) available at http://www.ibtimes.co.uk/articles/508882/20130925/edward-snowden-nsa-scandal-swift-tftp-eu.htm

[52] CRS Report, http://www.fas.org/sgp/crs/row/RS22030.pdf

[53] *See generally* Gabriel Schoenfeld, *Necessary Secrets: National Security, the Media, and the Rule of Law* (2010) at 121.

[54] Bret Stephens, "The Age of American Impotence," Wall Street Journal June 25, 2013 available at http://online.wsj.com/news/articles/SB10001424127887324637504578565530512048940

[55] http://www.usatoday.com/story/theoval/2013/07/04/obama-merkel-snowden-surveillance-leaks/2488927/

during the August 2013 G-20 Summit in Russia during which tensions about Snowden's extradition and asylum status were unresolved.[56]

In addition to diplomatic relationships, United States' intelligence agencies have extensive relationships with foreign intelligence services. Not only will diplomatic interactions be more difficult, but the intelligence relationships will be challenges as well. U.S. intelligence has good relations with many foreign intelligence services despite what one may read in the press during periods of heightened intelligence interest.

The Director of National Intelligence has the authority to establish intelligence arrangements with foreign governments.[57] The Director of the Central Intelligence Agency has a mandate to "conduct foreign intelligence liaison relationships with intelligence or security services of foreign governments or international organizations…."[58] The Director of the Defense Intelligence Agency is also required to "conduct foreign defense intelligence liaison relationships and defense intelligence exchange programs with foreign defense establishments, intelligence or security services of foreign governments…."[59] The Director of the National Security Agency has a similar mandate: The Director of the National Security Agency shall "conduct foreign cryptologic liaison relationships…."[60]

Each of these mandated liaison relationships will likely suffer because of the recent disclosures. These relationships can sour if foreign public opinion becomes dissatisfied with U.S. activities that may occur in secret, but with the approval of other heads of state.

*Russia*. The disclosure of alleged intelligence collection may have shifted the balance of moral authority toward Moscow as global awareness of the reported NSA programs proliferated. Russian President Vladimir Putin has been emboldened by the Snowden revelations as illustrated by his actions concerning Syria since the first release of data by *the Guardian* on June 5, 2013.

Russia's goal in Syria before the release of the classified information was avoid a "Western-backed effort at coercive regime change."[61] Russia has been anxious about the popularity of Islamist groups in predominantly Sunni Muslim countries after the Arab Spring revolutions.[62] Russia attributes the growth of these groups to U.S. attempts to spread democracy throughout the Middle East.[63] Thus, President Putin's political motivations have traditionally been more about domestic stability than about expanding Russia's foreign influence.[64] There was much

---

[56] See generally http://www.cnbc.com/id/100989042 and http://www.cbsnews.com/8301-250_162-57596558/obama-reevaluating-summit-with-russia-after-snowden-asylum/

[57] EO12333, Section 1.3(b)(4)(A)

[58] EO12333 Section 1.7(a)(5)

[59] EO12333 Section 1.7 (b)(5)

[60] EO12333 Section 1.7 (c)(8)

[61] Samuel Charap and Jeremy Shapiro, "How the US Can Move Russia on Syria," Al-Monitor, (July 22, 2013) available at http://www.al-monitor.com/pulse/originals/2013/07/syria-russia-geneva-engagement-peace-process-us-interests.html

[62] Fiona Hill, The Survivalist in the Kremlin, Project Syndicate (Jul. 4, 2013) available at http://www.project-syndicate.org/commentary/putin-s-rigid-approach-to-protecting-russia-by-fiona-hill

[63] Fiona Hill.

[64] According to Brookings Institute Senior Fellow Cliff Gaddy, "The whole point of their policy on Syria is that they are trying to protect themselves. What they are afraid of is instability. … Not really caring that much about who is in

speculation about how the events in Syria would be addressed by the G-20 summit. Analysts reported that Putin may not engage the topic. "He may not even, at the summit, engage in any major rhetorical condemnation of [chemical weapons use in Syria]. I think he may just let it, let the events speak for themselves."[65]

Despite this anxiety, Russia was relatively subdued on Syria until after the Snowden revelations. Emboldened by the growing global discontent with the U.S., Putin became more vocal on Syria and on U.S. foreign policy. His most dramatic maneuver was to publish an opinion article in the New York Times on September 11, 2013. According to Fiona Hill, of the Brookings Institute:

> Russian President Vladimir Putin has done it again, grabbing American and international attention with his *New York Times* op-ed cautioning the United States against the use of force in Syria, and scolding America for considering itself exceptional. Putin's piece has been met with surprise and outrage in the U.S., but its basic message has resonated with groups opposed to a unilateral U.S. strike against regime of Syrian President Bashar al-Assad. Putin has put himself right where he wants to be, at the top of the headlines on Syria, and writing the script for where the United States will have to take the crisis next: Back to the United Nations.[66]

Other circumstances concerning Syria undoubtedly helped encourage Putin to be more vocal, [67] but Russia is viewed by many as having taken the diplomatic high ground against President Obama's threat of military force. It is not difficult to interpret Putin's emboldened message, since he was considering - and then granted - temporary asylum to Edward Snowden while the debate on Syria was taking shape.

*European Union*. Traditional strong diplomatic and intelligence sharing relationships with members of the European Union have also been strained by revelations of programs allegedly collecting the personal communication of 35 heads of state.[68] These reports of U.S. surveillance

---

power as long as the people in power in the country control the forces within their borders as best they see. ... I don't think that he has a plan [for Syria] but the overall plan is somehow to protect Russia from the bad things that are happening." (http://www.brookings.edu/blogs/brookings-now/posts/2013/08/28-what-will-russia-do-if-us-strikes-syria).

[65] The Brookings Institute, U.S.-RUSSIA REPORTER ROUNDTABLE, 11 (August 29, 2013) available at http://www.brookings.edu/~/media/research/files/interviews/2013/08/29%20us%20russia%20relations/us%20russia%20relations%20g20%20syria%20arms%20control.pdf

[66] Fiona Hill, "Lessons in Communication from Vladimir Putin," msnbc (September 14, 2013) available at http://www.msnbc.com/msnbc/lessons-communication-vladimir-putin#discussions

[67] "F irst came the British parliamentary vote blocking Prime Minister David Cameron's initiative to join any U.S. military assault. Then came U.S. President Barack Obama's decision to put the issue to a vote before a reluctant Congress. The French government announced that -- unlike in Mali -- it would not go it alone in Syria. And United Nations Secretary-General Ban Ki-moon stated that the chemical weapons inspection team he had dispatched to Syria would need time to complete its work before determining whether there was sufficient evidence for the UN to approve the use of force." (http://www.brookings.edu/research/opinions/2013/09/06-putin-scores-syria-hill)

[68] James Ball, The Gurdian, NSA monitored calls of 35 world leaders after US official handed over contacts," (October 24, 2013) available at http://www.theguardian.com/world/2013/oct/24/nsa-surveillance-world-leaders-calls.

in Europe are "eating away at the fabric of trust that is part of the alliance."[69] According to the Council on Foreign Relations Senior Fellow Charles A. Kupchan , there is a direct relationship between the political discomfort with alleged U.S. intelligence collection and European disappointment about the President's inability to better balance security and civil liberties. Kupchan has noted that many Europeans feel that Obama "has failed to deliver on his pledge to clean up some of the excesses left behind by the George W. Bush administration." [70]

German Chancellor Angela Merkel originally defended the apparent intelligence cooperation disclosed by Snowden. She pointed out that Germany had "avoided terrorist attacks thanks to information from allies." But, in the face of new disclosures, she is now discussing limits on intrusions on privacy. Berlin has alluded repeatedly to "Cold War" tactics and has said spying on friends is unacceptable. Her spokesman has said a transatlantic trade deal requires a level of "mutual trust." [71] Chancellor Merkel has been criticized for her apparently feigned indignation about alleged cooperation with the U.S. intelligence community. "Germany has demanded explanations for Snowden's allegations of large-scale spying by the NSA, and by Britain via a programme codenamed 'Tempora', on their allies including Germany and other European Union states, as well as EU institutions and embassies."[72]

The Head of Germany's domestic intelligence has said he knew nothing about the reported NSA surveillance. Opposition parties believe otherwise. They claimed that, because German intelligence activities are coordinated within the Office of the Chancellor, high-level officials must have known about speculative NSA activities. [73] *Der Spiegel* has reported that NSA monitored about 20 million German phone connections and 10 million internet sessions on an average day and 60 million phone connections on above average days.[74] Thus, unconfirmed U.S. intelligence activities are now an issue that will affect German political leadership and the diplomatic and intelligence relationships between Germany and the U.S.

The impact on European Union allies is already seen in the talks being held between EU member states and the US about American surveillance tactics that may have included spying on European allies.[75] President Obama assured Germany that the United States "takes seriously the concerns of our European allies and partners."[76]

---

[69] Council on Foreign Relations, Interview of Charles A. Kupchan "U.S. Spying Casts Shadow Over Atlantic Alliance" October 29, 2013 available at https://secure.www.cfr.org/europe/us-spying-casts-shadow-over-atlantic-alliance/p31745

[70] Council on Foreign Relations, Interview of Charles A. Kupchan "U.S. Spying Casts Shadow Over Atlantic Alliance" October 29, 2013 available at https://secure.www.cfr.org/europe/us-spying-casts-shadow-over-atlantic-alliance/p31745

[71] http://www.sott.net/article/263704-Merkels-public-indignation-a-scam-Snowden-says-Germans-and-other-Western-states-in-bed-with-NSA.

[72] Merkel's public indignation a scam: Snowden says Germans and other Western states in bed with NSA

[73] http://www.sott.net/article/263704-Merkels-public-indignation-a-scam-Snowden-says-Germans-and-other-Western-states-in-bed-with-NSA.

[74] http://www.sott.net/article/263704-Merkels-public-indignation-a-scam-Snowden-says-Germans-and-other-Western-states-in-bed-with-NSA.

[75] http://www.usatoday.com/story/theoval/2013/07/04/obama-merkel-snowden-surveillance-leaks/2488927/

[76] Laura Smith-Spark**,** EU envoys meet over claims of U.S. spying on European allies CNN available at http://www.cnn.com/2013/07/04/world/europe/europe-us-spying/

The initiation of a dialogue between the U.S. and EU Members about intelligence collection and appropriate oversight[77] will also complicate the transatlantic relationship. Restrictions or legislation that shifts standards of privacy and data protection will diminish American and EU security.

*France*. Tensions in the European Union are not only limited to Germany. Although not as vocal, the French government has expressed concerns about U.S. intelligence activity because of the Snowden leaks. In response to allegations that NSA had collected "more than 70 million phone calls in France over a 30-day period," U.S. Ambassador to France Charles Rivkin was called meet with French diplomats.[78] A news release from French President Francois Hollande's office said he expressed his "deep disapproval with regard to these practices" and that "such alleged activities would be unacceptable between allies and friends."[79]

French indignation aside, the disclosures suggest a greater level of French involvement in global electronic surveillance. According to *the Guardian*, the Snowden materials contain high praise for the U.K's GCHQ's French partner, the General Directorate for External Security (DGSE). The French are reported to be a "highly motivated, technically competent partner, who have shown great willingness to engage on [internet protocol] issues, and to work with GCHQ on a 'cooperate and share' basis."[80] French media, too, has reported that DGSE is involved in the alleged collection. In early November, *La Jeune Politique* reported on the strained relations between Washington, D.C. and Paris. An article published by *Le Monde*, "detailed "the nature of the NSA's probing into France and…reported that data on over 70.3 million phone calls and SMS messages had been recorded by the NSA within a 30-day span." These reports "threw diplomatic relations into question and prompted a visit by Secretary of State John Kerry."[81]

American officials also noted the compliance of foreign intelligence services in the collection programs. According to NSA Director Keith B. Alexander, the documents released by Snowden "didn't represent data collected by the NSA or any other U.S. agency and didn't include records from calls within those countries."[82] In congressional testimony, Alexander noted that the data "were instead from a system that contained phone records collected by the U.S. and North Atlantic Treaty Organization countries 'in defense of our countries and in support of military

---

[77] http://www.usatoday.com/story/theoval/2013/07/04/obama-merkel-snowden-surveillance-leaks/2488927/

[78] Ed Payne and Khushbu Shah, "Report: U.S. intercepts French phone calls on a 'massive scale,' CNN October 21, 2013 available at http://www.cnn.com/2013/10/21/world/europe/france-nsa-spying/

[79] Ed Payne and Khushbu Shah, "Report: U.S. intercepts French phone calls on a 'massive scale,' CNN October 21, 2013 available at http://www.cnn.com/2013/10/21/world/europe/france-nsa-spying/

[80] Julian Borger, GCHQ and European spy agencies worked together on mass surveillance, The Guardian, 1 November 2013 available at http://www.theguardian.com/uk-news/2013/nov/01/gchq-europe-spy-agencies-mass-surveillance-snowden

[81] Grace Jamieson, French Intelligence DGSE Implicated in Snowden NSA Leaks *La Jeune Politique* November 9, 2013 available at http://lajeunepolitique.com/2013/11/09/french-intelligence-dgse-implicated-in-snowden-nsa-leaks/

[82] ADAM ENTOUS and SIOBHAN GORMAN, "Europeans Shared Spy Data With U.S," The Wall Street Journal, Oct. 29, 2013 available at http://online.wsj.com/news/articles/SB10001424052702304200804579165653105860502

operations.'"[83] He said the conclusion that the U.S. collected the data is incorrect. "And it's false that it was collected on European citizens. It was neither."[84]

The disclosures – and comments from the U.S. government - put French leaders in a difficult political position. Despite their initial vocal protest of U.S. intelligence activities, now it appears as if the French intelligence services were not only in on the collection, but also provided the data to their American and British partners. According to U.S. Secretary of State John Kerry, "France is one of the U.S.'s closest allies" and that France and the U.S. "work together to protect the security of their citizens."[85] If these claims are accurate, then it is safe to assume the collaboration and sharing of intelligence goes beyond those activities illegally disclosed by Snowden.

Assuming that the French do provide intelligence assistance to and data sharing with NATO, GCHQ, and NSA, the political pressures may be so strong as to curtail that assistance and sharing. If the media reports about French technical collection capability, the positive GCHQ assessment of French intelligence abilities, and General Alexander's statements about the reasons for intelligence relationships are all true, then any reduction in intelligence and data sharing will reduce the effectiveness of French, U.K, EU, NATO, and U.S. intelligence operations. If the current pressures result in less sharing or more restricted information exchanges between France and the U.S., then it is U.S. national security is impacted.

Some predict that the discomfort with the public disclosure of critical intelligence activities will result in the establishment of new norms of intelligence-gathering within the Atlantic Alliance. Rules such as "no snooping on officials above a certain level; or no significant intelligence gathering without informing the intelligence agency of the other side" are being considered.[86] There is current legislation in the European parliament that seeks to "tighten privacy laws and make it more difficult for Europeans to share information with non-European companies like Google and Facebook."[87] This will make intelligence more difficult and more expensive to collect, also impacting U.S. national security.

*Latin America*. Snowden's illegal disclosures have impacted U.S. national security by weakening foreign relations not only with Russia and Europe, but also in Latin America. Threats to U.S. national security from Latin America remain significant. "Economic stagnation, high rates of violent crime and… ruling party efforts to manipulate democratic institutions to consolidate power, and slow recovery from natural disasters are challenging [security measures]."[88]Countries

[83] Adam Entous and Sioban Gorman , "Europeans Shared Spy Data With U.S," The Wall Street Journal, Oct. 29, 2013 available at http://online.wsj.com/news/articles/SB10001424052702304200804579165653105860502
[84] Adam Entous and Sioban Gorman, "Europeans Shared Spy Data With U.S," The Wall Street Journal, Oct. 29, 2013 available at http://online.wsj.com/news/articles/SB10001424052702304200804579165653105860502
[85] Ed Payne and Khushbu Shah, "Report: U.S. intercepts French phone calls on a 'massive scale,' CNN October 21, 2013 available at http://www.cnn.com/2013/10/21/world/europe/france-nsa-spying/
[86] Council on Foreign Relations, Interview of Charles A. Kupchan "U.S. Spying Casts Shadow Over Atlantic Alliance" October 29, 2013 available at https://secure.www.cfr.org/europe/us-spying-casts-shadow-over-atlantic-alliance/p31745.
[87] Council on Foreign Relations, Interview of Charles A. Kupchan "U.S. Spying Casts Shadow Over Atlantic Alliance" October 29, 2013 available at https://secure.www.cfr.org/europe/us-spying-casts-shadow-over-atlantic-alliance/p31745.
[88] WWT at 26.

hostile to the U.S., such as Iran, have been expanding their influence in Latin America and the Caribbean.[89]

Threats from illicit narcotics trafficking emanate primarily from the Western Hemisphere. Mexico and Colombia are source countries for the majority of illegal drugs consumed in the United States, according to the Director of National Intelligence. Illicit trafficking continues to undermine U.S. security. Some of the highest violent crime rates are found in Honduras, El Salvador and Guatemala. "In addition, weak and corrupt institutions in these countries foster permissive environments for gang and criminal activity, limit democratic freedom, encourage systemic corruption, and slow recovery."[90] National security threats are abundant in Latin America, and recent illegal disclosures of classified information will not help diplomatic or intelligence sharing relationships with permissive or corrupt governments.

The disclosures have impacted U.S. national security relationships with Latin America, but particularly Brazil. Good intentions over the past three years to establish a trade deal and Brazilian membership in the UN Security council have been unsuccessful. Brazil's President Dilma Vana Rousseff has stated that each country has much to gain from deepening coordination with the U.S. It is reasonable to assume that given the threats to stability and the illicit narcotics trafficking from Latin America, that the U.S. intelligence Community has a partnership with Brazil. If true, then the disclosures by Snowden will complicate this cooperation. According to the *New York Times*, "Diplomatic ties have also been damaged, and among the results was the decision by Brazil's president, Dilma Rousseff, to postpone a state visit[91] to the United States in protest over revelations that the agency spied on her, her top aides and Brazil's largest company, the oil giant Petrobras."[92] Although an apology[93] may be enough to have a trade deal between the U.S. and Brazil reenergized, other issues continue to strain the relationship between Washington and Brasília.

According to the Council of Foreign Relations, the Snowden scandal, the White House "response to it and President Dilma Rousseff's decision to cancel the state visit has revealed the weakness of the U.S.-Brazil relationship."[94] Snowden's disclosures are now spawning an effort within Latin America to strengthen protections against alleged NSA collection. "According to the AP, Brazilian Foreign Minister Luiz Alberto Figueiredo said, 'We're going to talk with our partners,

---

[89] President Ahmadinejad traveled to the region twice in 2012. Tehran has cultivated ties to leaders of the Venezuelan-led Alliance for the Peoples of our Americas (ALBA) in Bolivia, Cuba, Ecuador, Nicaragua, and Venezuela, and maintains cordial relations with Cuba and Nicaragua. Relations with Tehran offer these governments a way to stake out independent positions on the international issue of Iran, while extracting financial aid and investment for economic and social projects. (WWT at 26)

[90] WWT at 26

[91] Rousseff was due to make a formal state visit to Washington…to meet U.S. President Barack Obama and discuss a possible $4 billion jet-fighter deal, cooperation on oil and biofuels technology, as well as other commercial agreements. (http://www.reuters.com/article/2013/09/04/us-usa-security-snowden-brazil-idUSBRE98314N20130904).

[92] Eric Schmitt and Michael Schmidt, Qaeda Plot Leak Has Undermined U.S. Intelligence, September 29, 2013 available at http://www.nytimes.com/2013/09/30/us/qaeda-plot-leak-has-undermined-us-intelligence.html?pagewanted=all&_r=0.

[93] http://www.reuters.com/article/2013/09/04/us-usa-security-snowden-brazil-idUSBRE98314N20130904.

[94] http://www.cfr.org/brazil/dear-president-dilma/p31379.

including developed and developing nations, to evaluate how they protect themselves and to see what joint measures could be taken in the face of this grave situation.'"[95]

Not only is U.S. national security affected by reactions in Brazil, but U.S. commercial interests as well. According to the LA Times, President Rousseff is "promoting legislation that would require technology companies such as Google and Facebook to store data collected in Brazil on Brazilian soil and therefore submit it to Brazilian law."[96] In addition, Brazil is now planning to develop a secure e-mail system to improve the security of government communications against American spying. Ironically, "President Dilma Rousseff used the secure messaging channel Twitter to make the announcement that she's going to order SERPRO – that country's federal data processing service – to implement a whole-of-government secure e-mail system."[97]

The reaction in Brazil over the illegal disclosures about alleged surveillance illustrates the diplomatic impact of the disclosure of classified information. The relationships with Latin American trade and diplomatic partners will continue to be tense because of the Snowden leaks. Snowden's actions will continue to degrade critical U.S. diplomatic and information sharing relationships.[98] According to the *National Security Strategy*, the "strategic partnerships and unique relationships we maintain with Canada and Mexico are critical to U.S. national security and have a direct effect on the security of our homeland."[99]

*Pakistan.* The U.S. relationship with Pakistan has been "tragic and tormented."[100] The country's internal instability, complex tribal dynamics, and political ideology have threatened U.S. security and international peace. Pakistan's rapidly growing population, "nuclear arsenal, and relationships with China and India will continue to force it onto the United States' geostrategic map in new and important ways over the coming decades."[101] With respect to diplomatic relations with the U.S., Islamabad is primarily concerned with Afghanistan and the consequences of the rapidly shrinking U.S. military presence.[102]

The Obama Administration claims that Al Qa'ida's remains centered in Pakistan and that this core "remains the most dangerous component of the larger network…."[103] Threats to U.S. national security will increase if the country's governance and security regress to historical levels, if the Taliban maintains control of sections of Afghanistan, and al-Qa'ida is not

---

[95] Peter Grier, "Are Edward Snowden NSA leaks messing up US foreign relations," Christian Science Monitor September 3, 2013 available at http://www.csmonitor.com/USA/DC-Decoder/Decoder-Wire/2013/0903/Are-Edward-Snowden-NSA-leaks-messing-up-US-foreign-relations.

[96] Kathleen Hennessey and Vincent Bevins, "Brazil postpones state visit to U.S. over Snowden spying leaks," LA Times *September 17, 2013, available at* http://www.latimes.com/world/worldnow/la-fg-wn-ff-brazil-us-edward-snowden-spying-leaks-20130917,0,5186201.story#axzz2jmpqWim6.

[97] Richard Chirgwin," Brazil whacks PRISM with secure email plan," The Register, October 14, 2013 available at http://www.theregister.co.uk/2013/10/14/brazil_waxes_lyrical_on_security/

[98] Peter Grier, "Are Edward Snowden NSA leaks messing up US foreign relations," Christian Science Monitor September 3, 2013 available at http://www.csmonitor.com/USA/DC-Decoder/Decoder-Wire/2013/0903/Are-Edward-Snowden-NSA-leaks-messing-up-US-foreign-relations.

[99] National Security Strategy at 42.

[100] Daniel Markey, "No Exit from Pakistan," CFR available at http://www.cfr.org/pakistan/no-exit-pakistan/p31250

[101] Daniel Markey, "No Exit from Pakistan," CFR available at http://www.cfr.org/pakistan/no-exit-pakistan/p31250

[102] See generally WWT at 18.

[103] NSS at 20.

neutralized. According to the *National Security Strategy*, "To prevent future attacks on the United States, our allies, and partners, we must work with others to keep the pressure on al-Qa'ida and increase the security and capacity of our partners in [Afghanistan and Pakistan]."[104]

Beyond the Al Qa'ida threat, the Director of National Intelligence is concerned about the future economic issues in Pakistan. With a very limited tax base, poor tax collection system, and reliance on U.S. foreign aid, the country has no promise of economic growth. These economic circumstances can encourage corruption and the acceptance of terrorist groups who provide much needed currency.[105]

It is undeniably wise to collect intelligence in regions from which these types of national security threats can originate. According to the *Washington Post*, there are intelligence gaps concerning the security of Pakistan's nuclear program, chemical and biological weapons capabilities, and the "loyalties of counterterrorism sources recruited by the CIA."[106] These concerns are so pervasive budget documents are reported to divide the world into two illicit weapons categories: Pakistan and everybody else.[107]

An illegally disclosed summary of the U.S. intelligence community's budget allegedly indicates a significant increase in intelligence activities against Pakistan. This increase may indicate a substantial level of distrust of Pakistan. "They also reveal a more expansive effort to gather intelligence on Pakistan than U.S. officials have disclosed."[108] This belief is supported by Husain Haqqan a former Pakistani ambassador to the United States: "If the Americans are expanding their surveillance capabilities, it can only mean one thing. The mistrust now exceeds the trust."[109] The loss of trust can complicate cooperation with Pakistan intelligence services, restrict intelligence sharing between the two countries, and thus reduce the security of both the U.S. and Pakistan.

The Snowden disclosures are undermining an already tense relationship between the U.S. and Pakistan. The illegal disclosures will likely reduce intelligence sharing and military cooperation at time when threats for both countries are still existential. The disclosures have diminished U.S.

---

[104] NSS at 20

[105] WWT at 18

[106] Greg Miller, Craig Whitlock and Barton Gellman, "Top-secret U.S. intelligence files show new levels of distrust of Pakistan," The Washington Post, September 2 available at http://www.washingtonpost.com/world/national-security/top-secret-us-intelligence-files-show-new-levels-of-distrust-of-pakistan/2013/09/02/e19d03c2-11bf-11e3-b630-36617ca6640f_print.html

[107] Greg Miller, Craig Whitlock and Barton Gellman, "Top-secret U.S. intelligence files show new levels of distrust of Pakistan," The Washington Post, September 2 available at http://www.washingtonpost.com/world/national-security/top-secret-us-intelligence-files-show-new-levels-of-distrust-of-pakistan/2013/09/02/e19d03c2-11bf-11e3-b630-36617ca6640f_print.html

[108] Greg Miller, Craig Whitlock and Barton Gellman, "Top-secret U.S. intelligence files show new levels of distrust of Pakistan," The Washington Post, September 2 available at http://www.washingtonpost.com/world/national-security/top-secret-us-intelligence-files-show-new-levels-of-distrust-of-pakistan/2013/09/02/e19d03c2-11bf-11e3-b630-36617ca6640f_print.html

[109] Greg Miller, Craig Whitlock and Barton Gellman, "Top-secret U.S. intelligence files show new levels of distrust of Pakistan," The Washington Post, September 2 available at http://www.washingtonpost.com/world/national-security/top-secret-us-intelligence-files-show-new-levels-of-distrust-of-pakistan/2013/09/02/e19d03c2-11bf-11e3-b630-36617ca6640f_print.html.

national security by damaging the diplomatic and intelligence relationship with a key ally in a region from whence one of the greatest attacks against the U.S. originated.

The diplomatic and intelligence relationships established over the past sixty years have been critical to the security of the United States. National security is proportionally linked to cooperation with other nations. The quantity and quality of intelligence sharing with foreign intelligence services can reduce the burden and expense on U.S intelligence agencies. Regardless of the veracity of the information illegally disclosed by Snowden, the tensions it is causing within foreign relations must negatively impact the intelligence sharing and cooperation. Less sharing and cooperation equals reduced national security for the U.S.

Intelligence relationships with foreign security services support good partnerships between the U.S. and the partner nation. These relationships provide access to areas the U.S. may not have direct admission. Partners can offer intelligence agility with an ability to collect information that may take longer in the U.S. They provide local insight to a particular target of areas with expertise not resident in the U.S. intelligence community. And relationships with foreign intelligence services may provide cover for U.S. interests by masking American action under their domestic security or military organizations.[110] These advantages have been placed at risk by the recent disclosures of potentially classified information.

**Commercial**

Diplomatic and intelligence cooperation between nations is vital to U.S. national security, but so too is the cooperation between the private and public sectors within the United States. Policy and technology developments over the past sixty years have diminished the capacity of the U.S. government to establish the state-of-the-art technology. This has not always been the case. According to the Intelligence and National Security Alliance:

> Throughout the history of U.S. intelligence, there has been a necessary partnership between government, the private sector, and academia to enhance research, development, manufacturing, and fielding of systems that support the intelligence mission. A broad range of innovations including the earliest computers and dynamic spaceborne collection systems resulted from this partnership.
>
> Through careful attention and nurturing of these partnerships, impressive cutting-edge technologies were developed and utilized on projects including the U-2, SR-71, CORONA overhead collection systems and the CRAY supercomputers.[111]

[110] Rosenbach, Eric and Aki Peritz. "Intelligence and International Cooperation." Memorandum, "Confrontation or Collaboration? Congress and the Intelligence Community," Belfer Center for Science and International Affairs, Harvard Kennedy School, July 2009 available at http://belfercenter.ksg.harvard.edu/publication/19153/intelligence_and_international_cooperation.html

[111] Intelligence and National Security Alliance, "Critical Issues for Intelligence Acquisition Reform: Industry's Assessment of the Intelligence Community Acquisition Process," 1 (October 2008) available at http://www.insaonline.org/i/p/a/i/d/a/Index.aspx?hkey=d73d5c3e-80a5-492b-9fd5-2f7caab8b8da.

Most major defense contractors claim to support intelligence programs throughout the intelligence community.[112] Because the U.S. national security apparatus apparently depends so heavily on the private sector, any damage to that relationship will have a corresponding negative impact on national security. It appears as if the illegal disclosures by Snowden are diminishing national security by causing a rift between high-tech firms and NSA.

A recent letter sent by six leading technology companies is an example of this rift. On October 31, 2013 Facebook, Google, Apple, Yahoo, Microsoft and AOL urged the White House to "work with Congress in addressing…critical reforms that would provide much needed transparency and help rebuild the trust of Internet users around the world."[113] These companies evidently believe that current surveillance practices require re-examination:"Our companies believe that government surveillance practices should also be reformed to include substantial enhancements to privacy protections and appropriate oversight and accountability mechanisms for those programs."[114]

This call for reform – perhaps motivated more by corporate interests than national security interests – may result in less access to information, less cooperation between the public and private sectors, and more bureaucratic demands on the intelligence community when accessing data that has little or no impact on the privacy of U.S. citizens. As noted by the first Assistance Secretary for Policy at the Department of Homeland Security and former General Counsel at the National Security Agency Steweart Baker, "In the long run, any effective method of ensuring privacy is going to have to focus on using technology in a smart way, not just trying to make government slow and stupid."[115] Companies such as Facebook, Google, Apple, Yahoo, Microsoft and AOL handle so much global data and continue to create new ways with which to connect, it is unwise to undermine any speculative partnership with these and similar private companies. Information sharing is already a challenging enough issue for the public and private sectors.

The same principles described by the 9/11 Commission report concerning information within the government, apply to information sharing between the government and the private sector:

> But the security concerns need to be weighed against the costs. Current security requirements nurture overclassification and excessive compartmentalization of information among agencies. Each agency's incentive structure opposes sharing, with risks…but few rewards for sharing information. There are no punishments for not sharing information. Agencies uphold a need-to-know culture of

[112] See generally Booz Allen Hamilton, http://www.boozallen.com/consulting/view-our-work; Northrop Grumma, http://www.northropgrumman.com/capabilities/Pages/default.aspx; Lockheed Martin, http://www.lockheedmartin.com/us/what-we-do/emerging.html; General Dynamics, http://www.gd-ais.com/.
[113] Facebook, Google, Apple, Yahoo, Microsoft and AOL, Letter to The Honorables Leahy, Lee, Conyers, Sensebrenner, October 31, 2013 available at http://sensenbrenner.house.gov/uploadedfiles/usa_freedom_act_letter_10-31-13.pdf.
[114] Facebook, Google, Apple, Yahoo, Microsoft and AOL, Letter to The Honorables Leahy, Lee, Conyers, Sensebrenner, October 31, 2013 available at http://sensenbrenner.house.gov/uploadedfiles/usa_freedom_act_letter_10-31-13.pdf.
[115] Stewart Baker, *Skating on Stilts: Why we aren't stopping tomorrow's terrorism* 314 (2010). Baker's book has enlightened commentary on the privacy issue

> information protection rather than promoting a need-to-share culture of integration.[116]

The current version of the ideas described more than 10 years ago could be that data available to corporations is overly protected and excessively compartmented within the private sector. Each company and government agency should incentivize sharing when national security is at risk. There should be liability for not providing information, rather than liability protections for sharing information with the U.S. government. Both public and private sectors must adopt a culture of integration.

The most recent and likely legislation promoting insufficient, but improved information sharing was S. 2105, The Cybersecurity Act of 2012. This bill – like many other before it – failed to become law because of mutual mistrust between the government and private sector and a suspicion of mutual incompetence.[117] Enhanced information sharing, whether under S. 2105 or any other bill, would have contributed to national security. Because of the disclosures by Snowden, there is now no appetite in Washington to pursue any information exchange between the national security apparatus and corporate America.

According to the *Washington Post*, "The tone of industry reaction to the NSA revelations has grown more aggressive since the first stories appeared in *The Washington Post* and Britain's *Guardian* newspaper in June. Companies that initially were focused on defending their reputations gradually began criticizing the government and challenging it in court. Some companies also have worked to harden their networks against infiltration. A turning point came with the *Washington Post* revealed an NSA program that collects user information from Google and Yahoo as it moves among data centers overseas. To some, this amounted to a degree of intrusiveness that, though speculated about by privacy activists, was beyond what many in the industry thought possible."[118]

The national security impact is clear: less cooperation between the U.S. national security departments and agencies will result in less or more difficult access to data and less or more difficult access to technical innovation.

**Public Confidence**

The American National Security Strategy "begins with a commitment to build a stronger foundation for American leadership, because what takes place within our borders will determine our strength and influence beyond them."[119] What is taking place within our borders in response to the disclosures of potentially classified information is reducing U.S. national security by undermining public confidence in the National Security Agency, the Intelligence Community,

---

[116] 9/11 Commission Report at 417.

[117] See generally, Charles Abbott, "Cybersecurity bill dead after second U.S. Senate rebuff," Reuters Nov 14, 2012, available at http://www.reuters.com/article/2012/11/15/us-usa-cyber-legislation-idUSBRE8AE04720121115.

[118] Craig Timberg and Ellen Nakashima, "Amid NSA spying revelations, tech leaders call for new restraints on agency," (October 31, 2013) available at http://www.washingtonpost.com/world/national-security/amid-nsa-spying-revelations-tech-leaders-call-for-new-restraints-on-agency/2013/10/31/7f280aec-4258-11e3-a751-f032898f2dbc_print.html.

[119] NSS at 2.

and the federal government. The daily media indictments of one of the premier intelligence agencies in history is disrespectful to the thousands of American citizens who work at NSA, and has presented the public with an inaccurate image of intelligence community oversight. The loss of public trust resulting from amateur media analysis and by Snowden's actions is already damaging national security by distracting national security professionals from their jobs. In our democracy, reductions in public support and agency credibility will inevitably result in fewer resources, reduced authority, and additional scrutiny. For students of national security history, this portends a pendulum swing back to less information sharing, less authority to collect intelligence vital to U.S. national security, and a reversion to less sharing of information within the U.S. government and with foreign allies.

According to a Pew Research poll conducted shortly after the first illegal disclosures by *the Guardian*, "for the first time since 9/11, Americans are now more worried about civil liberties abuses than terrorism."[120] According to Pew, 56 percent of Americans believe U.S. federal courts have inadequately limited counter-terrorism telephone and internet data collection by the government. "An even larger percentage (70%) believes that the government uses this data for purposes other than investigating terrorism."[121] This data show the misunderstanding of the value of the alleged NSA programs, despite congressional testimony and declassified documents that demonstrate that these programs have stopped violent attacks against the U.S. and its allies. Regardless of the value of the disclosed activities, the political reaction has been swift.

President Obama announced in early August that reforms were coming for NSA surveillance. Section 215 of the USA Patriot Act and the role of the Foreign Intelligence Surveillance Court are now under review. "Obama wants to let a civil liberties representative weigh in on the court's deliberations to ensure that an adversarial voice is heard and will form a high-level group of outside experts to review the U.S. surveillance effort."[122] The president has also ordered the declassification of many documents surrounding the collection of data in the hope of restoring the public trust damaged by the recent disclosures.

Congress has also announced its own reforms. The Intelligence Oversight and Surveillance Reform Act[123], introduced by Senators Ron Wyden, Mark Udall, Richard Blumenthal, and Rand Paul, will "prohibit bulk collection of Americans' records, shield Americans from warrantless searches of their communications and install a constitutional advocate to argue significant cases before the secret Foreign Intelligence Surveillance court."[124] No action has been taken on the bill since its introduction on September 25, 2013.

---

[120] Glenn Greenwald, "Major opinion shifts, in the US and Congress, on NSA surveillance and privacy," The Guardian July 26, 2013 available at http://www.theguardian.com/commentisfree/2013/jul/29/poll-nsa-surveillance-privacy-pew.

[121] Pew Research Center for People and the Press, "Few See Adequate Limits on NSA Surveillance Program," July 26, 2013 available at http://www.people-press.org/2013/07/26/few-see-adequate-limits-on-nsa-surveillance-program/.

[122] Steve Holland And Jeff Mason," Obama says reform ahead for NSA surveillance program," Milwaukee Wisconsin Journal Sentinel, August 9, 2013 available at http://www.jsonline.com/news/usandworld/obama-begins-news-conference-addresses-nsa-b9972397z1-219024921.html

[123] S. 1551 available at https://www.govtrack.us/congress/bills/113/s1551/text

[124] Senator Ron Wyden, "Surveillance Reform Package Ends Bulk Collection of Phone Records; Creates Constitutional Advocate for Secret Court," Press Release, September 25, 2013 available at

Congress has also considered an amendment to the Defense Appropriations bill that would restrict NSA's access to data.[125] It was the first legislative challenge to programs that the White House, the Office of the Director of National Intelligence, the Department of Justice, and the National Security Agency have claimed have stopped violent attacks against the U.S. The amendment was defeated by 12 votes in the House of Representatives sending a clear message to the Obama Administration that there is anxiety about the program. "Though the amendment barely failed, the vote signaled a clear message to the NSA: we do not trust you."[126]

The Snowden disclosures may also have larger implications for other elements of the U.S. government. As a consequence of the disclosures, Congress and the executive branch are considering placing a political appointee at the head of the National Security Agency and separating the roles of Director, NSA and Commander, U.S. Cyber Command. According to the *Washington Post*, "National Security Council officials are scheduled to meet soon to discuss the issue of separating the leadership of the National Security Agency and Cyber Command, a shift that some officials say would help avoid an undue concentration of power in one individual and separate entities with two fundamentally different missions: spying and conducting military attacks. The administration is also discussing whether the NSA should be led by a civilian."[127]

With the reduction in potential legal authority for NSA, public sentiments against the NSA surveillance that has contributed so much to national security and the pressures that are a consistent feature of budget negotiations, can reductions to the NSA budget be far behind? With less money, less authority, and less credibility, NSA will wind up with fewer people, less data, and impoverished contributions to national security. According to top agency counsels, reforms under consideration may reduce Americans privacy in an effort to enhance it. Lawyers from the Intelligence Community are now arguing against certain reforms, in support of the status quo.[128]

Perhaps it was inevitable that the national security apparatus constructed since 9/11 would be dismantled when Americans no longer view the threat to the U.S. as starkly as they did on September 11, 2001. With political dysfunction, government shutdown, unemployment, perhaps al-Qaeda, Iran's nuclear program, Muslim extremism, and nuclear proliferation are no longer worth allowing the NSA to access metadata.

---

http://www.wyden.senate.gov/news/press-releases/surveillance-reform-package-ends-bulk-collection-of-phone- records-creates-constitutional-advocate-for-secret-court

[125] See generally, Justin Amash, Amash NSA Amendment Fact Sheet July 24, 2013 available at http://amash.house.gov/speech/amash-nsa-amendment-fact-sheet

[126] http://www.theguardian.com/commentisfree/2013/oct/25/nsa-no-congress-oversight

[127] Ellen Nakashima, "U.S. weighs option to end dual leadership role at NSA, Cyber Command," Washington Post November 6, 2013 available at http://www.washingtonpost.com/world/national-security/us-weighs-proposal-to-end-dual-leadership-role-at-nsa-cyber-command/2013/11/06/e64a23d8-4701-11e3-b6f8-3782ff6cb769_story.html.

[128] John Hudson, "Top Obama Lawyers: Reforming the NSA Could Hurt Americans' Privacy," Foreign Policy blog November 4, 2013 available at http://thecable.foreignpolicy.com/posts/2013/11/04/top_obama_lawyers_reforming_the_nsa_could_hurt_americans_privacy_rights.

As noted by lawyer, diplomat, writer, and philosopher Joseph de Maistre, "Every nation gets the government it deserves."[129] If the citizens of the American republic demand a reduction in their own security as a result of actions taken in violation of laws their representatives established, then we will not only get the government we deserve, but also the level of security we have chosen.

**Conclusion**

Regardless of the legitimacy, or lack thereof, of Snowden's actions, the material he has revealed in violation of law, regulation, and oath has placed U.S. security at risk. The disclosures have resulted in significant damage to diplomatic relationships with countries that share intelligence with the U.S., domestic commercial relationships between the U.S. public and private sectors leading to less information sharing and innovation, and damage to the public confidence in the NSA leading to fewer resources and authority to protect the U.S. in the manner that it has done so since 9/11. The disclosures will also facilitate operational changes in the behavior of current adversaries' practices and attention to the protection of their information; the damage to It will become more difficult, more expensive, and more time consuming to collect and analyze information on terrorist groups, foreign governments, and foreign militaries.

Our Republic is resilient and will survive the exposure of the "plumbing" of NSA's intelligence apparatus.[130] Surviving will be more dangerous, more expensive, and take more time than reforms would have required absent Snowden's illegal activities. Just as Snowden must do on his own, we must all ask ourselves if the transparency that he has forced onto the system is worth the diminishing of American security.

[129] Bartlett's Roget's Thesaurus, 2003,

[130] See generally comments from Michael V. Hayden during the Washington Post Live's Cyber Summit, 3 October 2013 avaiable at http://www.washingtonpost.com/postlive/conferences/cybersecurity-2013

Preliminary Draft – Please Do Not Cite Without Permission
To be Published in *I/S: A Journal of Law and Policy for the Information Society*
9 ISJLP ___ (2014).
http://www.is-journal.org

# Secret without Reason and Costly without Accomplishment: Questioning the NSA's Metadata Program

John Mueller[*]
Mark G. Stewart[**]

When Edward Snowden's revelations emerged in June 2013 about the extent to which the National Security Agency was secretly gathering communications data as part of the country's massive 9/11-induced effort to catch terrorists, the administration of Barack Obama set in motion a program to pursue him to the ends of the earth in order to have him prosecuted to the full extent of the law for illegally exposing state secrets.

However, the President has also said that the discussions about the programs these revelations have triggered have actually been a good thing: "I welcome this debate. And I think it's healthy for our democracy. I think it's a sign of maturity because probably five years ago, six years ago, we might not have been having this debate."[1]

There may be something a bit patronizing in the implication that the programs have been secret because we weren't yet mature enough to debate them when they were put into place.

---

[*] Ralph D. Mershon Senior Research Scientist, Mershon Center for International Security Studies and Adjunct Professor, Department of Political Science, Ohio State University, and Senior Fellow, Cato Institute.

[**] ARC Australian Professorial Fellow, and Professor and Director, Centre for Infrastructure Performance and Reliability The University of Newcastle, New South Wales, Australia.

[1] Office of the Press Secretary, The White House, *Statement by the President*, June 7, 2013, Fairmont Hotel, San Jose, California.

Setting that aside, however, a debate is surely to be welcomed—indeed, much overdue. It should be conducted not only about the National Security Agency's amazingly extensive data-gathering programs to amass information on telephone and e-mail conversations—programs that have, according to the President, included "modest encroachments" on privacy—but also more generally about the phenomenal expansion of intelligence and policing efforts in the wake of 9/11.[2]

As Dana Priest and William Arkin have documented in their the remarkable book, *Top Secret America*, by 2009 there were something like 1,074 federal government organizations and almost 2,000 private companies devoted to counterterrorism, homeland security, and intelligence spread over more than 17,000 locations within the country. At least 263 of these were created or reorganized after 9/11.[3] A simple listing of the government's "Special Operations Programs" runs to 300 pages.[4] Collectively this apparatus launched far more covert operations in the aftermath of 9/11 than it had during the entire Cold War.[5]

A comparison might be useful. Since 9/11, 53 cases have come to light of Islamist extremist terrorism, whether based in the United States or abroad, in which the United States itself has been, or apparently has been, targeted.[6] The total number of real terrorists, would-be

---

[2] White House, *Statement by the President*, June 7, 2013.

[3] Dana Priest and William M. Arkin, *Top Secret America: The Rise of the New American Security State* (New York: Little, Brown, 2011), 86.

[4] Priest and Arkin, *Top Secret America*, 25-26.

[5] Priest and Arkin, *Top Secret America*, 12.

[6] See John Mueller (ed.), *Terrorism Since 9/11: The American Cases* (Columbus, OH: Mershon Center, Ohio State University, 2013).

terrorists, and putative terrorists populating this set of cases, excluding FBI and police undercover operatives, is less than 100. Thus, the United States has created or reorganized *three entire counterterrorism organizations* for every terrorist arrest or apprehension it has made of people plotting to do damage within the country.

Although much of discussion in this paper can be extrapolated more widely, it focuses primarily—and for starters—on one of the two surveillance programs revealed by Snowden. These two programs have often been mixed in, or confused, with each other.[7]

One of them, Prism, somewhat more commonly known from its section in the law as 702, permits NSA to gather electronic communication information on e-mail and phone conversations after approval by a judge if the target is both outside the United States and not an American citizen and if there is an appropriate and documented foreign intelligence purpose for the collection.

The other, known as 215, authorizes the gathering in bulk of business and communication records within the United States. It has been used in particular to amass telephone billing records—numbers called, numbers received, and conversation length—for every telephone in the

In principle, the 215 data are only supposed to be collected if there are "reasonable grounds to believe" the records are "relevant" to a terrorist investigation of a "known or unknown" terrorist organization or operative. Creatively expanding the word, relevant, to the breaking point, it has been taken in practice to mean that NSA can gather billing records for

---

[7] A useful discussion of the two programs is Walter Pincus, "NSA should be debated on the facts," washingtonpost.com, July 29, 2013. On "known or unknown," see the Opinion of Judge Claire V. Eagan, United States Foreign Surveillance Court, Washington, DC, Docket BR 13-109, 2013.

every telephone conversation in the country. As many, including Senator Patrick Leahy, have pointed out, this broad approach could also be applied to banking, credit card, medical, financial, and library records, all of which could be held as reasonably to be somehow "relevant" to the decidedly wide-ranged quest to catch terrorists.

The information gathered by either program can be held for five years.

This paper primarily deals with the 215 program, the more controversial of the two, the one that involves the massive gathering of telephone billing records, or "metadata," within the United States.

In the debate that has burgeoned since Snowden's revelations, a number of questions have been raised about the civil liberties and privacy implications of NSA's massive surveillance efforts. This paper focuses on three additional questions. None of these is terribly legalistic, but they are questions about the surveillance program that ought to be given more thorough examination.

The first two—why was the program secret and how much does it cost?—seem never to come up even though they are crucial if we are going to have an adult conversation on the issue. The third—what has the program accomplished?—has attracted some attention, but it clearly needs much more, and this paper examines it in the broader context of the obsessive, and massively expensive, efforts by police and intelligence since 9/11 to deal with the threat that is envisioned to be presented by terrorism, a quest that has involved following literally millions of leads that go nowhere.[8]

---

[8] For commentary on the often-bizarre quality of this quest, see John Mueller and Mark G. Stewart, "The Terrorism Delusion: America's Overwrought Response to September 11," *International Security,* Vol. 37, No. 1 (Summer 2012): 81–110.

## 1. Why was the 215 program secret?

Under Executive Order 135256, classification is permitted if "disclosure of the information reasonably could be expected to result in damage to the national security, which includes defense against transnational terrorism." The order continues: "If there is significant doubt about the need to classify information, it shall not be classified."[9] There is also a classification level of top secret. As defined in Executive Order 12356, top secret is "applied to information, the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to national security."[10]

It is difficult to see how earlier exposure of the program's existence would have damaged national security, gravely or otherwise.[11] No one seems to be saying that the Snowden documents put undercover intelligence operatives or operations overseas or elsewhere in danger of being exposed, or that they reveal military secrets about weapons, or that they compromise United States strategy or tactics. Instead, we get such vague, atmospheric pronouncements to the press as that from outgoing FBI Director Robert Mueller in August 2013: "Mueller said that leaks by former NSA contractor Edward Snowden 'have impacted, and [are] in the process of impacting, capabilities around the world,' but when asked to expand on this, he said simply, 'No

---

[9] Jim Harper, John Mueller, and Mark Stewart, *Comments on Notice of Proposed Rulemaking: Passenger Screening Using Advanced Imaging Technology, TSA-2013-0004 (RIN 1652-AA67)*, Cato Institute, June 21, 2013, 13.

[10] Priest and Arkin, *Top Secret America*, 10n.

[11] Actually, as will be discussed more fully in section 2, the program was essentially outed in an article in *Wired* in 2012 based on information supplied by a former NSA official. However, the program's existence was firmly denied by people in charge. The later release of the Snowden materials settled the matter.

details.'"[12] Even less helpful has been the expression of "belief" promulgated by NSA chief Keith B. Alexander: "Based on what we know to date, we believe these disclosures have caused significant and irreversible harm to the security of the nation."[13]

In fact, of course, terrorists have surely known at least since the 1990s (when Osama bin Laden ceased talking on a satellite phone) that United States intelligence is searching communications worldwide to track them down.[14] Year after year we have heard about "chatter" that has been picked up by official agencies, and one certainly has to conclude that it has dawned on the chatterers that there are extensive efforts to listen in. The terrorists may not know the precise number, but they are likely to be at least dimly aware—and are unlikely to be surprised—that the NSA, in its tireless quest to conduct its very global war on terror intercepts and ingests 1.7 billion communication elements every day. These include, note Priest and Arkin, "telephone calls, radio signals, cell phone conversations, emails, text and Twitter messages, bulletin board postings, instant messages, website changes, computer network pings, and IP addresses."[15] It is possible, but unlikely, that the current revelations will impress the terrorists even further about the extent of the surveillance effort. But even if that is so, the effect would mainly be to make their efforts to communicate even more difficult and inconvenient.

Conceivably, as some maintain, there still exist some exceptionally dim-witted terrorists

---

[12] Billy Kenber, "Outgoing Director Robert S. Mueller, III tells how 9/11 reshaped FBI mission," *Washington Post*, August 22, 2013.

[13] Shane Harris, "The Cowboy of the NSA," foreignpolicy.com, September 9, 2013.

[14] Mary Lu Carnevale, "Tracking Use of Bin Laden's Satellite Phone," Washington Wire, blogs.wsj.com, May 28, 2008.

[15] Priest and Arkin, *Top Secret America*, 77.

or would-be terrorists who are oblivious to the fact that their communications are rather less than fully secure. But such supreme knuckle-heads are surely likely to make so many mistakes—like advertising on Facebook or searching there or in chatrooms for co-conspirators—that sophisticated and costly communications data banks are scarcely needed to track them down.[16]

Some defenders of the program have creatively argued that exposure of the 215 program has aided terrorists because they now know that NSA is gathering only metadata on telephone calls in the United States, not their content.[17] But, if terrorists or other bad people read past the first paragraph in discussions of the 215 program, they surely can also note that, if information gathered is deemed suspicious, investigators can apply for legal authority to record the content of the communications. And they can do that readily as well in the 702 program which gathers and monitors not only metadata, but also content. Moreover, like many others, terrorists are likely to suspect that, despite prominent denials to the contrary, considerably more than metadata is

---

[16] See, for example, cases 16, 30, 39, 40, 41, 48, 51, and 52 in Mueller, *Terrorism Since 9/11*.

[17] Thus General Michael Hayden on "Meet the Press," NBC, June 16, 2013: "What I fear al-Qaeda learns about this program is not what we're *allowed* to do but they learn what we're *not* allowed to do, and they learn the limits of the program." Asked on CBS' "Face the Nation" on June 30, 2013, about what harm had been done, Hayden said, "Three things. Number one: Operational things have been disclosed. I mean you're a newsman, you know about protecting sources and methods and here now our sources and methods have been made public, so that's one. Second: Look, we cooperate with a lot of governments around the world. They expect us to be discreet about that cooperation. I can't imagine a government anywhere on the planet who now believes we can keep a secret." He was never given an opportunity to divulge the third as his impatient interviewer rushed to move on. The second "harm" is a relevant concern for programs that are secret, but it is scarcely relevant to the issue of why the program was made secret in the first place.

gathered even under the 215 program.[18]

It is also argued that the program was kept secret in order to protect the private communications companies, like AT&T, Verizon, and Sprint, that are dutifully supplying the NSA with data. If their customers find out that their billing records are being handed over to the government, it is said, they might drop their service and migrate to a company that doesn't send its data to the NSA. However, the potential embarrassment of businesses is not usually deemed to constitute a threat, grave or otherwise, to national security. Moreover, the concern certainly appears to have been overwrought: the Snowden disclosures do not seem to have led to mass customer defections from cooperating companies. In part, perhaps, this is because it is difficult to find out which companies do not hand data over. Moreover, even if one could find out, the company to which the customer defects could at any time be forced to turn over its data anyway.

Unkind people might suggest that the real reason these programs were kept secret actually stems from the administration's fear that public awareness of their "modest encroachments" on privacy would make further efforts to encroach more difficult.

Thus Reuters notes that a former Air Force secretary ominously warns that a "growing unease about domestic surveillance could have a chilling effect on proposed cyber legislation that calls for greater information-sharing between government and industry." And it also notes that,

---

[18] For example, when former NSA agent William Binney, was asked if he believed that the government was only collecting metadata, he responded, "Well, I don't believe that for a minute. OK? I mean, that's why they had to build Bluffdale, that facility in Utah with that massive amount of storage that could store all these recordings and all the data being passed along the fiberoptic networks of the world. I mean, you could store 100 years of the world's communications here. That's for content storage. That's not for metadata. Metadata, if you were doing it and putting it into the systems we built, you could do it in a 12- by-20-foot room for the world. That's all the space you need. You don't need 100,000 square feet of space that they have at Bluffdale to do that." PBS NewsHour, August 1, 2013.

since the revelations, more lawmakers have signed on to legislation that would strengthen the privacy protections in the 1986 Electronic Communications Privacy Act.[19] Perhaps, then, the programs were kept secret not so much to protect people from terrorism, but to protect the government from the annoying and inconvenient public and Congressional outcry that, as it happens, constitutes the untidy stuff of democracy.

The degree to which classification has been overdone is suggested more generally by the case of Bradley Manning who downloaded hundreds of thousands of classified documents that were subsequently made public by Wikileaks in 2010. As it turned out, these documents, while embarrassing to some officials, contained no really significant new disclosures—just about all the information was already essentially public, though in many cases it was less textured and nuanced.[20] Although prosecutors forcefully argued in Manning's military trial that he was guilty of "aiding the enemy"—surely the key issue in determining whether something should be classified—the judge failed to find him guilty on that charge.[21] If Manning's disclosures failed to "aid the enemy," it would be difficult to argue that Snowden's revelations, which are primarily about methods of data collection that were already known and/or easy to surmise, would be of much aid either.

**2. How much does the 215 program cost?**

---

[19] Andrea Shalal-Esa and Joseph Menn, "U.S. domestic spying controversy complicates cybersecurity efforts," Reuters, June 8, 2013.

[20] Editor Bill Keller of the *New York Times*, conversation with John Mueller, Berkeley, California, April 9, 2011.

[21] 21 Charlie Savage, "Manning is Acquitted of Aiding the Enemy," *New York Times*, July 30, 2013.

If we are now to have a healthy debate about 215, NSA's stupendous megadata program, it seems reasonable to suggest that debaters should be supplied with information about how much the program costs. This information would furnish a key starting point for any debate.

Presumably, that figure has thus far been classified because the program itself was classified. But now that we know only too well that the program exists, why should its cost remain secret?

It is certainly difficult to see how knowing that cost would help the terrorists—except perhaps to amaze them further. However, there is the danger, of course, that the cost of gathering and storing and evaluating huge amounts of metadata on the telephone conversations of all Americans might also amaze American taxpayers. Perhaps that's another reason why the programs have been kept secret.

It's possible as well that the cost figure for the program remains undisclosed in part because no one actually knows how much the program costs. This may seem a strange observation, but, as an example, the Department of Homeland Security has set up a vast array of "Fusion Centers" to police terrorism, but is unable to determine how much they cost. It estimates that somewhere between $289 million and $1.4 billion were awarded for the Centers between 2003 and 2010—an uncertainty gap of over a billion dollars that is impressive even by Washington standards.[22]

That this phenomenon is widespread is suggested by Priest and Arkin. In researching their

---

[22] Majority and Minority Staff Report, *Federal Support for and Involvement in State and Local Fusion Centers*, Permanent Subcommittee on Investigations, Committee on Homeland Security and Governmental Affairs, United States Senate, October 3, 2012, 3. See also John Mueller, "Confusion: What if we can't catch terrorists in America because there aren't any?" foreignpolicy.com, October 8, 2012.

book, they discovered that the spending increases on counterterrorism in the aftermath of 9/11 often took place so fast and so chaotically that no one was able to keep a count of the costs. As they put it strikingly,

> American taxpayers have shelled out hundreds of billions of dollars to turn the machine of government over to defeating terrorism without ever really questioning what they were getting for their money. And even if they did want an answer to that question, they would not be given one, both because those same officials have decided it would gravely harm national security to share such classified information—and because the officials themselves don't actually know.[23]

**Program, investigatory, and opportunity costs**

The direct costs of maintaining the 215 program might be quite low. However, a full accounting should include not only the actual cost of gathering and storing the surveillance data, but also the costs of constantly sorting through it to generate and develop leads. According to the NSA's director of compliance, the agency queries its databases about 20 million times each month.[24] Presumably that includes both databases and, equally presumably, it involves a great deal of human interaction, all of which must be paid for.

Costs should also include those involved in following up the leads once they have been generated, an issue to be discussed in the next section.

Also included in the tally should be the opportunity costs: what else could the money have been used for? For example, it has often been noted that there has been a downgrading by the FBI and other agencies of other priorities, including the pursuit of white collar crime like fraudulent banking practices, to focus on the pursuit of (substantially non-existent) terrorists: as

---

[23] Priest and Arkin, *Top Secret America*, xviii-xix.

[24] Charlie Savage, "N.S.A. Calls Violations of Privacy 'Minuscule'," nytimes.com, August 16, 2013.

an assistant U.S. attorney put it in 2002, "This is a great time to be a white-collar criminal."[25] To fully evaluate the costs of the NSA surveillance efforts, one would need to take this issue into account.

**Privacy costs: the issue of trust**

In addition, some consideration should be made for the less quantifiable costs of privacy invasion and for the potential misuse of the data.

Although the program has built-in safeguards, its operation ultimately requires us to trust those in charge. Citing unpleasant historical precedents from the days of Richard Nixon and J. Edgar Hoover and from the runup to the Iraq War of 2003, Stephen Walt has arrestingly suggested, or warned, that the program could be used to intimidate or harass whistle-blowers, dissidents, and overly-inquisitive journalists: "once someone raises their head above the parapet and calls attention to themselves by challenging government policy, they can't be sure that someone inside government won't take umbrage and try to see what dirt they can find."[26]

The current administration's credibility on the issue of whether it can be trusted not to abuse this system has already has been strained to the point that, in a Rasmussen poll in June 2013, 57 percent of the respondents deemed it likely that the government would use data dredged up by the NSA to harass political opponents.[27]

---

[25] Sarah Chayes, "Blinded by the war on terrorism," *Los Angeles Times*, July 28, 2013.

[26] Stephen Walt, "The real threat behind the NSA surveillance programs," foreignpolicy.com, June 10, 2013.

[27] "57% Fear Government Will Use NSA Data to Harass Political Opponents," Rassmussen Reports, June 13, 2013. See also Eugene Robinson, "We can handle the truth on

That wary reaction has been enhanced by the fact that officials have several times been caught in lies—or supreme exercises in Clintonian sophistry—about the NSA programs.

There is, for example, the response of NSA director Alexander to a March 2012 cover story in *Wired* magazine that reported the views of William Binney, a formet NSA official.

Binney left the agency in late 2001 when it launched its warrantless-wiretapping program, but, according to the article, he retained close contact with other agency employees for several years thereafter. "They violated the Constitution setting it up," he says, "But they didn't care. They were going to do it anyway, and they were going to crucify anyone who stood in the way. When they started violating the Constitution, I couldn't stay." Binney contended that, without a warrant, the NSA was collecting "a vast trove of international and domestic billing records" from major American telephone companies and that "they're storing everything they gather."[28]

In the ensuing months, Alexander blithely denied Binney's contention. "To think we're collecting on every US person…that would be against the law…. The fact is we're a foreign intelligence agency."[29] He also categorically insisted that "we don't hold data on U.S. citizens," a statement that has been defended by the administration on the grounds that the NSA's internal definition of "data" does not include "metadata"—a language-stretching nuance Alexander neglected to mention when he made his statement. As it happens, however, the agency's actual

---

NSA spying," *Washington Post*, July 3, 2013.

[28] James Bamford, "The NSA Is Building the Country's Biggest Spy Center (Watch What You Say)," *Wired*, March 15, 2012.

[29] James Bamford, "They Know Much More Than You Think," *New York Review of Books*, August 15, 2013.

internal definition of "data" *does* specifically include "call event records and other Digital Network Intelligence metadata."[30] In like manner, Alexander probably had a special private definition of "dossier" in mind when he vehemently stated in 2012 that the notion that the NSA has "millions or hundreds of millions of dossiers on people is absolutely false."[31]

Then, in March 2013, Director of National Intelligence James Clapper was asked in a Senate Intelligence Committee hearing, "Does the NSA collect any type of data at all on millions or hundred of millions of Americans?" He replied, "No, sir…. Not wittingly." The Senator asking the question says it had been sent to Clapper's office the day before and that Clapper was given a chance to amend his answer. After Snowden's revelations three months later spectacularly shattered Clapper's crisp denial (as well as Alexander's earlier ones), Clapper sent a letter to the Committee stating that his answer had been "clearly erroneous" and that when responding he imagined that the question referred to content, not metadata which he somehow believes the NSA does not collect "wittingly." Clapper has also said that an honest response would have required him to divulge secrets that were highly classified, and thus he came up with the "least untruthful" answer he could imagine at the time.[32]

There is additional evidence of deception in the disclosure that the NSA illegally collected email content data on thousands, or tens of thousands, of Americans before that

---

[30] Barton Gellman, "NSA broke privacy rules thousands of time per year, audit finds," *Washington Post*, August 15, 2013.

[31] Ellen Nakashima and Joby Warrick, "For NSA chief, terrorist threat drives passion to 'collect it all,' observers say," *Washington Post*, July 14, 2013.

[32] Robinson, "We can handle the truth on NSA spying." See also Bamford, "They Know Much More Than You Think."

practice was closed down by the courts in 2011.[33] The court's opinion on this was classified, and the Obama administration fought a Freedom of Information lawsuit seeking to get it released.[34] In the wake of the Snowden disclosures, however, the opinion was finally declassified and released in heavily redacted form. In it, the judge specifically points out that he had previously been the victim of "a substantial misrepresentation regarding the scope of a major collection program" and that the information gathered had been "fundamentally different from what the court had been led to believe."[35]

Similar concerns were raised in a 2009 ruling that had originally been classified as top secret—that is, deemed to be information "the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to national security." The ruling concerned the way the NSA probed phone numbers on an "alert list." When it was finally declassified under pressure in 2013, the ruling included declarations that the government had failed to comply with the court's orders and had compounded this by "repeatedly submitting inaccurate descriptions of the alert process" and that court-approved privacy safeguards had "been so frequently and systematically violated" that they "never functioned effectively." A senior official explained rather lamely, but entirely plausibly, that any violations were "unintentional" because "there was nobody at N.S.A. who really had a full understanding of how the program was operating at the

---

[33] Ellen Nakashima, "NSA gathered thousands of Americans' e-mails before court struck down program," washingtonpost.com, August 21, 2013. See also Charlie Savage and Scott Shane, "Secret Court Rebuked N.S.A. on Surveillance," *New York Times*, August 21, 2013.

[34] Gellman, "NSA broke privacy rules."

[35] Ellen Nakashima, "NSA gathered thousands of Americans' e-mails."

time."[36]

It might be wondered, then, what *intentional* violations, keeping Walt's admonition in mind, could lead to. Senator Dianne Feinstein, who chairs the Senate Intelligence Committee, insists that her committee "has never identified an instance in which the NSA has intentionally abused its authority to conduct surveillance for inappropriate purposes." However, the agency's director of compliance, has indicated that there have been a very small number (perhaps one every five years) of "willful errors."[37]

Relevant as well to a discussion of credibility is the disclosure that in 2006 the NSA deliberately weakened an encryption standard accepted both nationally and internationally in a systematic effort to defeat privacy protections for Internet communications, a venture that compromised the National Institute of Standards and Technology in the process.[38]

In all this, an assessment of the privacy costs attendant on the NSA's surveillance efforts should hold in mind, to the degree to which they apply, warnings suggested in this passage from George Orwell's novel, *1984*:

> There was of course no way of knowing whether you were being watched at any given moment. How often, or on what system, the Thought Police plugged in on any individual wire was guesswork. It was even conceivable that they watched everybody all the time. But at any rate they could plug in your wire whenever they wanted to. You had to live— did live, from habit that became instinct—in the assumption that every sound you made was overheard, and, except in darkness, every movement scrutinized.[39]

---

[36] Scott Shane, "Court Upbraided N.S.A. on Its Use of Call-Log Data," *New York Times*, September 10, 2013.

[37] Savage, "N.S.A. Calls Violations of Privacy, 'Miniscule'"

[38] Shane, "Court Upbraided N.S.A. on Its Use of Call-Log Data."

[39] Quoted, Bamford, "They Know Much More Than You Think."

## 3. What has the 215 program accomplished?

Once one knows the cost of the program, one is in a position to weigh that figure against the benefit the program has generated. The President insists that the privacy-encroaching programs "help us prevent terrorist attacks" and therefore "on net, it was worth us doing."[40]

However, they are worth us doing only if their benefit, on net, outweighs their cost.[41] And that is a calculation that should be made, not simply declared.

**The 9/11 atmosphere: consequences and persistence**

To begin an appraisal of this issue, one must assess the program in context. It has been only one cog in the massive intelligence-gathering machine impelled by the trauma of 9/11. The trauma is certainly understandable. But the fears, and therefore the hasty and expensive actions they inspired, have clearly been substantially inflated. As anthropologist Scott Atran puts it, "Perhaps never in the history of human conflict have so few people with so few actual means and capabilities frightened so many."[42]

In the immediate aftermath of the September 11 attacks, recalls Rudy Giuliani, who was mayor of New York at the time, "anybody, any one of these security experts, including myself, would have told you on September 11, 2001, we're looking at dozens and dozens and multiyears

---

[40] White House, *Statement by the President*, June 7, 2013.

[41] For an introduction to this process with specific applications to counterterrorism policy, see John Mueller and Mark G. Stewart, *Terror, Security, and Money: Balancing the Risks, Benefits, and Costs of Homeland Security* (New York: Oxford University Press, 2011).

[42] Scott Atran, *Talking to the Enemy: Faith, Brotherhood, and the (Un)Making of Terrorists* (New York: Ecco, 2010), xiv. See also John Mueller, *Overblown* (New York: Free Press, 2006); Mueller and Stewart, "Terrorism Delusion."

of attacks like this."[43] Or, as journalist Jane Mayer observes, "the only certainty shared by virtually the entire American intelligence community" in the months after September 11 "was that a second wave of even more devastating terrorist attacks on America was imminent."[44]

The fears and concerns were, of course, plausible extrapolations from the facts then at hand. However, that *every* "security expert" should hold such erroneous views and that the intelligence community should be *certain* about them is fundamentally absurd. It was also an entirely plausible extrapolation from facts then at hand that 9/11 could prove to be an aberration rather than a harbinger.[45] Yet it appears that no one in authority could even imagine that proposition to be true even though it could have been taken to fit the available information fully as well as the passionately-embraced alarmist perspective.[46]

---

[43] Miles O'Brien and Carol Costello, interview with New York Mayor Rudy Giuliani, "Giuliani: 'Have to Be Relentlessly Prepared,'" CNN, July 22, 2005.

[44] Jane Mayer, *The Dark Side: The Inside Story on How the War on Terror Turned into a War on American Ideals* (New York: Doubleday, 2008), 3.

[45] John Mueller, "Harbinger or Aberration?" *National Interest*, Fall 2002, 45-50. John Mueller, "False Alarms," *Washington Post*, September 29, 2002. Russell Seitz, "Weaker Than We Think," *American Conservative*, December 6, 2004.

[46] In his book, *George F. Kennan*, John Lewis Gaddis, observes that no one at the summit of foreign policy in 1950 anticipated most of the major international developments that were to take place in the next half-century. Among these: "that there would be no World War" and that the United States and the USSR, "soon to have tens of thousands of thermonuclear weapons pointed at one another, would agree tacitly never to use any of them" (New York: Penguin, 2012, 403). However, the absence of further world war, whether nuclear or not, was compatible with the fairly obvious observation that those running world affairs after World War II were the same people or the intellectual heirs of the people who had tried desperately to prevent that cataclysm. It was entirely plausible that such people, despite their huge differences on many issues, would manage to be capable of keeping themselves from plunging into a self-destructive repeat performance. Although this perspective was not, of course, the only possible one, there was no definitive way to dismiss it, and it should accordingly have remained on the table. For the suggestion that, if *no one* anticipated this distinct possibility in 1950, the US might

At any rate, operating under that apparently unanimous mentality, US intelligence extravagantly imagined that the number of trained al-Qaeda operatives in the United States was between 2,000 and 5,000.[47] Terrorist cells, they told reporters, were "embedded in most U.S. cities with sizable Islamic communities," usually in the "run-down sections," and were "up and active" because electronic intercepts had found some of them to be "talking to each other."[48]

Over the years, such thinking has been internalized and institutionalized in a great many ways, and it has proved to be notably resistant to counter-information. Indeed, officials often seem to live in what might be called "I think, therefore they are" denial.[49] Thus, on February 11, 2003, a year and a half after 9/11, FBI Director Robert Mueller assured the Senate Intelligence Committee that "the greatest threat is from al-Qaeda cells in the US that we have not yet identified." He somehow judged the threat from those unidentified entities to be "increasing" and claimed to know that "al-Qaeda maintains the ability and the intent to inflict significant casualties in the US with little warning." On February 16, 2005, he testified before the same

---

have been better served if those at the summit of foreign policy had been replaced by coin-flipping chimpanzees who would at least occasionally get it right from time to time out of sheer luck, see John Mueller, "History and Nuclear Rationality," nationalinterest.org, November 19, 2012.

[47] Bill Gertz, "5,000 in U.S. Suspected of Ties to al Qaeda; Groups Nationwide Under Surveillance," *Washington Times,* July 11, 2002; and Richard Sale, "US al Qaida Cells Attacked," UPI, October 31, 2002.

[48] Sale, "US al Qaida Cells Attacked." Another account relayed the view of "experts" that Osama bin Laden was ready to unleash an "11,000 strong terrorist army" operating in more than sixty countries "controlled by a Mr. Big who is based in Europe," but that intelligence had "no idea where thousands of these men are." Andy Lines, "War on Terror: Bin Laden Army: 11,000 Terror Agents Set to Strike," *Mirror* (London), September 24, 2001.

[49] On this issue, see also Mueller and Stewart, "The Terrorism Delusion."

committee that he remained "very concerned about what we are not seeing," a sentence rendered in bold lettering in his prepared text.[50] By that time, however, an FBI report had concluded that, despite years of well-funded sleuthing, it had yet to uncover a single true al-Qaida sleeper cell in the United States. For some, or no, reason, this report was kept secret although it managed to be leaked.[51] However, some in the FBI remained unmoved, telling Fox News at the time that "just because there's no concrete evidence of sleeper cells now, doesn't mean they don't exist."[52]

Since the number of al-Qaeda operatives actually in the country came out to be zero or nearly so, and since the threat of terrorism in the country proved to be far more limited than initially feared—not even one of the "dozens and dozens" of attacks like 9/11 ever materialized of course—there might logically have been some judicious cutbacks to the funds devoted to dealing with the issue in subsequent years. However, despite the fact that initial perspectives have proven to have been much overblown, the FBI will continue to engage, perhaps forever, in the exhaustive, and exhausting, pursuit of terrorists in what some in the bureau call "ghost chasing."[53] Thus, Director Mueller: "I'll fight tooth and nail for more criminal agents, but I'll never at the end of the day take an agent out of counterterrorism and national security."[54]

---

[50] Director Mueller's testimony can be found at http://www.fbi.gov/congress/congress.htm.

[51] Brian Ross, "Secret FBI Report Questions Al Qaeda Capabilities: No 'True' Al Qaeda Sleeper Agents Have Been Found in U.S.," ABC News, March 9, 2005.

[52] "FBI Can't Find Sleeper Cells," Fox News, March 10, 2005.

[53] Garrett M. Graff, *The Threat Matrix: The FBI at War in the Age of Global Terror* (New York: Little, Brown, 2011), 398.

[54] Graff, *Threat Matrix*, 524.

Far overdue, clearly, are extensive and transparently-presented studies seeking rationally to evaluate the massive increases in homeland security expenditures that have taken place since 9/11—increases that total well over $1 trillion. But virtually none of this has been done by the administrators in charge.[55]

Instead, initial, if clearly alarmist, perspectives have been essentially maintained and the vast and hasty increases in spending on homeland security continue to be perpetuated. Important in this have been increases in intelligence and policing as the questing enterprise continues to be expanded, searching for the needle by adding more and more hay.

The NSA has been central to this expansion of course, but it is only part of the process.

For example, there are those Fusion Centers—clusters of state and local law enforcement people set up to collect intelligence on terrorist and other criminal activity in their area and then to send reports on their findings to DHS for evaluation. In 2012, DHS Secretary Janet Napolitano called them "one of the centerpieces of our counterterrorism strategy."[56]

Considerable hackles were raised by a 2012 report from the Permanent Subcommittee on Investigations of the Senate Committee on Homeland Security and Governmental Affairs that concluded the utility of the terrorism-related reporting from the Fusion Centers had been at best "questionable." Investigators shuffled through 610 Fusion Center intelligence reports submitted to DHS over a 13 month period. Of the 574 unclassified reports filed, 188 were "cancelled" by DHS reviewers generally because they contained "nothing of value" or simply failed to be devoid

---

[55] For a discussion, see Mueller and Stewart, *Terror, Security, and Money*, 1-9.

[56] R. Jeffrey Smith, "Senate Report Says National Intelligence Fusion Centers Have Been Useless," foreignpolicy.com, October 3, 2012.

of "any actual intelligence." While the overall cancellation rate for the reports was around 30 percent, nearly half of those dealing with terrorism were rejected out of hand. That didn't leave many. Of the 386 reports accepted, only 94—considerably less than two a week—related "in some way" to potential terrorist activity. Moreover, more than a quarter of these simply duplicated information already known to the FBI, and "some were based on information drawn from publicly available websites or dated public reports." One, in fact, simply relayed information from a Department of Justice press release that had been published months earlier.[57]

Moreover, continues the report, DHS has "struggled" to identify a clear example in which a Fusion Center provided intelligence that helped disrupt a terrorist plot. And, when investigators looked at the four "success stories" touted by DHS, they were "unable to confirm" that the Fusion Centers' contributions were "as significant as DHS portrayed them; were unique to the intelligence and analytical work expected of fusion centers; or would not have occurred absent a fusion center."[58]

However, it apparently never occurred to the investigators that the reason intelligence reporting on terrorists is so limited in quantity and so abysmal in overall quality is that there was virtually nothing to report. Absence of evidence, it implies, cannot possibly be evidence of absence. Accordingly, the report recommends that *even more* money should be spent on them.

Local intelligence reporting efforts, it suggests, should be reformed to eliminate

---

[57] Majority and Minority Staff Report, *Federal Support for and Involvement in State and Local Fusion Centers*. On hackles, see Smith, "Senate Report."

[58] Majority and Minority Staff Report, *Federal Support for and Involvement in State and Local Fusion Centers*, 83.

duplication, the training and numbers of intelligence reporters should be improved, and better efforts to evaluate their output should be put into place.[59]

Another instance of substantially unproductive hay-heaping is the establishment by the New York Police Department of a trademarked and extensively promoted "If You See Something, Say Something™" terrorism hotline. It has received tens of thousands of tips, but not one of these, it appears, has led to a terrorism arrest.[60]

For its part, the FBI celebrated (or acknowledged) the receipt of its 2 millionth terrorism tip from the public in August 2008.[61] There is no record whether these have been more productive than the tips supplied to the NYPD. However, they have all been dutifully scrutinized in the post-9/11 atmosphere under the admonition of Director Robert Mueller that "No counterterrorism lead goes uncovered."[62] Or, as the assistant chief for the FBI's National Threat Center puts it extravagantly, it's the lead "you don't take seriously that becomes the 9/11."[63]

The bureau has folded this information into a "Threat Matrix," an itemized catalogue of all the "threats"—or more accurately "leads"—needing to be followed up. As Garrett Graff

---

[59] Majority and Minority Staff Report, *Federal Support for and Involvement in State and Local Fusion Centers*, 106. On this issue, see also Mueller, "Confusion."

[60] John Mueller, "Terror Tipsters," The Skeptics blog, nationalinterest.org, January 24, 2012. Mueller and Stewart, *Terror, Security, and Money*, 162. Harvey Molotch, *Against Security* (Princeton, NJ: Princeton University Press, 2012), 54-55.

[61] Donna Leinwand, "Psst—Leads from Public to FBI Rise," *USA Today*, August 15, 2008.

[62] Graff, *Threat Matrix*, 579.

[63] Leinwand, "Psst—Leads from Public to FBI Rise."

explains, the government pursues "upwards of 5,000 threats per day."[64] The Threat Matrix, or selected excerpts from it, form the centerpiece of the two hours of briefings on terrorism the FBI director undergoes each day.[65] Impelled by what some have called "The 9/11 Commission Syndrome"—an obsession with the career dangers in failing "to connect the dots"—it is in no one's interest to cull the threats "because it was possible you'd cull the wrong threat and end up, after the next attack, at the green felt witness table before the next congressional inquiry."[66] Consequently, the Threat Matrix "tracks all the unfolding terrorist plots and intelligence rumors" and is "filled to the brim with whispers, rumors, and vacuous, unconfirmed information."[67] In result, "claims that ordinarily wouldn't have made it past the intake agent, claims that wouldn't even be written down weeks earlier, suddenly became the subject of briefs to the President in the Oval Office."[68]

Graff supplies an example. One entry in the Threat Matrix is crisply cited as "a threat from the Philippines to attack the United States unless blackmail money was paid." It turns out that this entry was based on an e-mail that said, "Dear America. I will attack you if you don't pay me 99999999999999999999999999999999999999999999 dollars. MUHAHAHA."[69]

---

[64] Graff, *Threat Matrix*, 399.

[65] Graff, *Threat Matrix*, 339.

[66] Graff, *Threat Matrix*, 400.

[67] Graff, *Threat Matrix*, 345. Also: "Every time the CIA picked up a squib of information, it tossed it into the Threat Matrix" (405).

[68] Graff, *Threat Matrix*, 344.

[69] Graff, *Threat Matrix*, 398. Graff says that the FBI dutifully ran down the e-mail's author and sent information to Philippine police who then paid a visit to the would-be

If, aided by the Threat Matrix, the government pursues some 5000 "threats" or leads each day, and if each lead takes an average of a half a week to investigate, the FBI has pursued some ten million of them over the years since 9/11—a process that has led to, at the very most, a few hundred prosecutions, most of them on quite minor charges.[70]

**The NSA: efforts and accomplishments**

In the panicky aftermath of 9/11, the National Security Agency, the institution of central concern here, has also expanded massively, and its computerized surveillance programs have been a central part of that process. As of 2011, the floor space it occupied matched that of the Pentagon, and its buildings are surrounded by 112 acres of parking space. There are plans to add 10,000 workers by 2026, and the price tag for just the first phase of this expansion is $2 billion.[71]71

It is important to evaluate what these programs have accomplished—to determine whether "on net" they have been "worth us doing" in their central mission of countering

---

extortionist's parents.

[70] Karen J. Greenberg (ed.), *Terrorism Trial Report Card: September 11, 2001-September 11, 2009*, New York University School of Law, Center on Law and Security, 2010. Moreover, whatever the ratio of needle to hay, living with the Threat Matrix seems to take a psychological toll on its daily readers. As Graff vividly describes the process, the Threat Matrix comes off as "a catalogue of horrors" (19), as the "daily looming prognoses of Armageddon" (489), and as "a seeming tidal wave of Islamic extremist anger that threatened to unhinge American society" (345). It could become "all-consuming and paralyzing" (345), and he quotes former CIA Director George Tenet: "You could drive yourself crazy believing all or even half of what was in it" (344). Or as another reader puts it, "Your mind comes to be dominated by the horrific consequences of low-probability events" (400). Obsessed by the implied imminence and certainty of doom, one overworked reader, Special Agent Brad Doucette, was led to commit suicide in 2003 (411). "Present fears," observes Macbeth, "are less than horrible imaginings."

[71] Priest and Arkin, *Top Secret America*, 74.

terrorism.

When asked in June 2013 at Senate hearings if NSA's massive data-gathering programs were "crucial or critical" in disrupting terrorist threats, the agency's head, General Alexander, doggedly testified that in "dozens" of instances the databases "helped" or were "contributing"—though he did seem to agree with the word "critical" at one point.[72] The key issue for evaluating the programs, however, given their costs and privacy implications, would be to determine not whether the huge databases were helpful or contributing, but whether they were necessary.[73]

After his testimony, Alexander provided Congress a list of terrorism cases in which his surveillance measures have help to disrupt terrorist plots or to identify suspects. The list reportedly numbers 54—unsurprisingly, the list itself is classified. On the surface, this seems to be an amazingly small number for several years' work. There have been hundreds of terrorism cases in the United States since 9/11. Some 53 of these, as noted earlier, have led to full-bore prosecutions for plotting to attack targets in the United States.[74] And there are dozens more that have led to prosecutions for sending, or plotting to send, support to terrorists overseas, while a few hundred have involved terrorism investigations that led to prosecutions on lesser charges.[75]

---

[72] CNN Newsroom, "Senate Investigates NSA Leak," June 12, 2013, transcript.

[73] NSA operatives sometimes suggest the program "ultimately completes the picture" or, in the words of FBI Deputy Director Sean Joyce, "closes the gap" on information on a case. These formulations ingeniously, if deceptively, create the impression that the information was necessary. Ellen Nakashima, "NSA cites case as success of phone data-collection program," *Washington Post*, August 8, 2013.

[74] See Mueller, *Terrorism Since 9/11*.

[75] The bulk of people convicted in "terrorism-associated" prosecutions, are sentenced to less than four years, and most of these less than one year. Federal inmates generally serve 85 percent of their sentences. Greenberg, *Terrorism Trial Report Card*, 13-14; see also 59.

There have also been hundreds—or perhaps even thousands—of terrorism cases overseas. If the NSA programs were so valuable, one would think that investigators on just about every case would routinely run their information by the NSA. Even if the NSA comes up blank, that would be helpful to know because it would close off some avenues of potential investigation that, if pursued, would have proven to be a waste of time and effort, allowing investigators to follow leads more likely to be productive.

That they apparently have not done so suggests either that investigators and prosecutors have only occasionally found the NSA to be a helpful ally or else that they were afraid that if they queried the NSA on the case at hand, the agency would spew out a raft of leads that would unproductively clutter and distract their investigation while greatly increasing its costs.

The experience at the FBI with NSA leads is likely relevant here. Explains Walter Pincus, if operatives at NSA, sorting through their 215 metadata collection or other sources, uncover "a questionable pattern" such as "calls to other suspect phones," they send a report to the FBI for investigation.[76] The FBI, then, is routinely supplied with what Graff calls "endless lists of 'suspect' telephone numbers." When followed up, these "leads" virtually never go anywhere: of 5000 numbers passed along, only 10—two-tenths of one percent—"panned out enough for the bureau to bother" to get court permission to follow them up. At the FBI, the NSA tips are often called "Pizza Hut" leads because, following them up, FBI agents "inevitably end up investigating the local pizza delivery guy." At one point, the generally diplomatic Robert Mueller bluntly told NSA director Alexander, "You act like this is some treasure trove; it's a useless time suck." An agent in the trenches puts it a bit less delicately: "You know how long it takes to chase 99 pieces

---

[76] Pincus, "NSA should be debated on the facts."

of bullshit?"[77]

This resonates with the experience of the CIA. Using its wealth of data, the NSA under Alexander has been fond of presenting massive, even supreme, exercises in dot-connecting in which hundreds or even thousands of people, places, and events are linked together in what some call BAGs, or "big ass graphs." For all their (presumed) awesomeness, these have reportedly produced very few useful leads. "I don't need this," said an exacerbated senior CIA official.

Because the BAGs include people who are three layers removed from the putative terrorist of interest, the number of people in any one full picture could number in the tens of millions.[78]

Even before coming to the NSA, Alexander had applied such massive data networks in the Army. Detractors say there was an absence of data and verifiable sources behind the leads, that a quarter of the people on the charts were already dead, and that about the only thing the people in the networks were connected to was, as it happens, "pizza shops."[79]

**The cases**

According to the testimony of an NSA official, of the 54 cases that were supposedly disrupted by NSA surveillance data, more than 90 percent involved 702 information.[80] Thus, 215 data presumably played a role in around 5 cases over the course of the program. According to General Alexander, only 13 of the 54 cases on the classified list had a "homeland nexus," the

---

77 Graff, *Threat Matrix*, 527.

78 Harris, "Cowboy of the NSA."

79 Harris, "Cowboy of the NSA."

80 Pincus, "NSA should be debated on the facts."

others having occurred in Europe (25), in Asia (11), and in Africa (5).[81]

Four of the cases, all presumably from the "homeland nexus" subset, were publically discussed on June 18, 2013, by Alexander and by Sean Joyce, Deputy Director of the FBI at the rather tendentiously titled "Hearing of the House Permanent Select Committee on Intelligence on How Disclosed NSA Programs Protect Americans, and Why Disclosure Aids Our Adversaries." Insofar as NSA surveillance played a role at all in these cases, it seems that it was the 702 program, not the 215 one, that was relevant.[82]

First, they suggested that the NSA programs helped apprehend an American who had done surveillance work (the value of which seems to have been fairly limited) for terrorist gunmen who killed 166 in a suicidal rampage in Mumbai, India, in 2008. He was later arrested as he was engaged in a plot to do terrorist damage in Denmark, a plot that was beset by many planning and financial difficulties at the time. According to *ProRepublica* reporter Sebastian Rotella who has done extensive research and reporting on the case, British intelligence already had the American under surveillance—suggesting that the Danish enterprise would never have been allowed to be carried out. The arrest resulted from a tip from the British, not from NSA intercepts. It does appear, however, that previously stored NSA intercepts, presumably from the 702 program, aided in building the legal case against the man.[83]

---

[81] Peter Finn, "NSA chief says surveillance programs helped thwart dozens of plots," *Washington Post*, June 27, 2013.

[82] Carlo Muñoz, "NSA chief cites 50 foiled plots in defense of spying program," *The Hill*, June 18, 2013.

[83] 83 Sebastian Rotella, "Did NSA Surveillance Help Thwart Plotter of Mumbai Attack?" www.pbs.org/wgbh/pages/frontline, June 12, 2013. See also Nick Gillespie, "Do the Zazi and Headley Arrests Prove the Power of NSA Total Surveillance?" reason.com, June 13,

The second case involves a San Diego cab driver from Somalia who has been convicted of sending the decidedly non-princely sum of $8,500 to help a designated terrorist group in Somalia fight Ethiopians who, with US support, had recently invaded the country. The government had been tapping his telephone for months, and Director Mueller appears to have singled out this case as the only one in which the collection of phone data had been "instrumental," a word, of course, that is not as strong as "crucial" or "critical" or "necessary."[84] Joyce says that an investigation of the potential case with 215 information that began in October 2007 "did not find any connection to terrorist activity," but that there was a breakthrough when NSA connected a San Diego number with a suspicious contact outside the country using 215.[85] However, it is not clear they needed any sort of data bank to sort through. Says Senator Ron Wyden, investigators had all the information they needed to get a court order to investigate.[86]

A correspondent for *The Hill* breathlessly characterizes the cab driver culprit as "a top terrorist financier in San Diego, who was supporting militant extremist groups in Somalia."[87] However, it certainly appears that the crime prosecuted at great effort and cost was, overall, a

---

2013. Joyce testified that the terrorist operative was uncovered "through 702 coverage of an al-Qaeda-affiliated terrorist." *Hearing of the House Permanent Select Committee on Intelligence on How Disclosed NSA Programs Protect Americans, and Why Disclosure Aids Our Adversaries*, Washington, DC: IC on the Record, Office of the Director of National Intelligence, June 18, 2013.

[84] Ken Dilanian, "NSA faces backlash over collecting phone data," latimes.com, July 27, 2013.

[85] 85 *Hearing of the House Permanent Select Committee on Intelligence.*

[86] Nakashima, "NSA cites case."

[87] Muñoz, "NSA chief cites 50 foiled plots."

rather trivial one.

The third case seems to be even more trivial. It involves three Muslim men, all naturalized American citizens, one in Kansas City and two in New York. At the time of the American invasion of Iraq in 2003, they decided they needed to fight for their "faith and community," in the words of one of them. Four years later, one of the men was able to connect to two apparently experienced al-Qaeda terrorists in Yemen. Hoping to join the fight in Iraq, Afghanistan, or Somalia, the American men sent money and equipment to their new friends in Yemen under the impression that these would be set aside for their military training. Over several months they sent thousands of dollars—one of them says it totaled more than $23,000— as well as watches, cold-weather gear, some Garmin GPS units, and a remote-controlled toy car. However, the recipients divided the physical loot among themselves and spent the money on (real) cars and as awards to families of Islamic martyrs. In 2008, the scam artists requested further payments of $45,000 which one of them planned to use to open an appliance store. They also suggested that the Americans were better suited to an operation in the United States and cajoled one of them into casing the New York Stock Exchange for a possible bombing—a "plot" that they never had any intention of carrying out, according to the testimony of one of them. The American did do a walk around the target, and then, several months later, submitted a one-page report on his adventure consisting of information that could have been gotten from Google maps and from tourist brochures. It was summarily trashed in disgust by his handlers.[88]

In his June 2013 testimony, Joyce said identification in the case was made not through

---

[88] Mark Morris, "Al-Qaeda bunco artist rolls terrorist from KC," *Kansas City Star*, June 29, 2013. $23,000: Mark Morris, "KC terrorist supported plan to bomb New York Stock Exchange, FBI tells Congress," *Kansas City Star*, June 18, 2013.

215, but through "702 authority."[89] At the same time, he raised interest, and then eyebrows, by dramatically proclaiming this to be a case "that was in the very initial stages of plotting to bomb the New York Stock Exchange." Another official said, "It was, as Deputy Director Joyce states, in its nascent stages and could have progressed well beyond that if it wasn't for our ability to obtain FISA material." However, when asked whether the plot was "serious," Joyce deftly dodged the issue: "I think the jury considered it serious because they were all convicted." As it happens, there were no jury trials: the three men all pleaded guilty and then only to providing support to terrorism, not to the NYSE plot (such as it was). According to the other official, FBI Deputy Director Joyce "misspoke."[90] Alexander nonetheless appears to have been delighted with Joyce's performance at the hearings. An open microphone reportedly captured him asking Joyce to tell his boss, FBI director Robert Mueller, "I own him another friggin' beer."[91]

Only the fourth case involves a serious potential for terrorism within the United States. This was the Zazi case of 2009 in which three Afghan-Americans received training in Pakistan before returning to the United States, plotting to set off bombs on the New York subway system.

Joyce testified that a connection was made through "702 authority."[92] But, as Justin

---

[89] *Hearing of the House Permanent Select Committee on Intelligence.* Ken McCarthy, "NSA chief says exposure of surveillance programs has 'irreversible' impact," theguardian.com, June 18, 2013.

[90] Brian Ross, Aaron Katersky, James Gordon Meek, and Lee Ferran, "NSA Claim of Thwarted Plot Contradicted by Court Documents," ABC News, June 19, 2013. See also John R. Harris, "FBI Concocted Bomb Plot Against NYSE to Mute NSA Surveillance Criticism," john.harris.io, June 25, 2013.

[91] Harris, "FBI Concocted Bomb Plot."

[92] *Hearing of the House Permanent Select Committee on Intelligence.*

Heilmann points out in a study of the episode and as others have more recently noted, the plot in the United States does not appear to have been disrupted so much by NSA data-dredgers, but rather by standard surveillance procedures implemented after the British provided a hot tip about Zazi based on his e-mail traffic to a known overseas terrorist address that had long been under surveillance.[93] At that point, US authorities had good reason to put the plotters on their radar and, as Senator Ron Wyden has pointed out, "the government had all the information it needed to go to the phone company and get an individual court order."[94] Having NSA's megadata collection might have been helpful, but it seems scarcely to have been required.

Actually, it is not clear that even the tip was necessary. Given the perpetrators' limited capacities, it is questionable whether the plot would have ever succeeded. For example, the plotters foolishly called attention to themselves by used stolen credit cards to purchase large quantities of potential bomb material thereby guaranteeing that the sales would be scrutinized and security camera information preserved. Moreover, even with his training and a set of notes at hand, Zazi, described by a step-uncle as "a dumb kid, believe me," *still* apparently couldn't figure it out, and he frantically contacted his overseas trainer for help several times. Each of these

---

[93] Justin Heilman, "Case 28: Zazi," in Mueller, *Terrorism Since 9/11*, 347-55. More recent: Ben Smith, "Public Documents Contradict Claim Email Spying Foiled Terror Plot," buzzfeed.com, June 7, 2013; British tip: "British Spies help prevent attack," *Telegraph*, November 9, 2009. It is conceivable that the 702 program, Prism, played a role in this process, but is not at all clear that this is so or that, if so, its role was necessary. For a discussion, see Dan Amira, "Did Controversial NSA Spy Programs Really Help Prevent an Attack on the Subway?" nymag.com, June 10, 2013. Alexander has said that 702 was "critical," but that 215 was not essential to the case: McCarthy, "NSA chief says exposure." See also Molotch, *Against Security*, 56, 58; Matt Apuzzo and Adam Goldman, *Enemies Within: Inside the NYPD's secret spying unit and bin Laden's Final Plot against America* (New York: Touchstone, 2013), 53-55; Gillespie, "Do the Zazi and Headley Arrests;" Dilanian, "NSA faces backlash."

[94] Nakashima, "NSA cites case."

communications was "more urgent in tone than the last," according to court documents.[95]

It was these communications that alerted the authorities.

When presenting his four cases at the Congressional hearings in June 2013, Alexander explained that he couldn't make the details of all the cases on his secret list public because "If we give all those out, we give all the secrets of how we're tracking down the terrorists as a community, and we can't do that."[96] The remaining 50 will remain shrouded in secret, then, presumably because it is believed that discussing them publicly would result in damage, perhaps even grave damage, to national security. Accordingly, so protected, we will never be able to examine them in our "healthy" debate on the issue of NSA surveillance.

Absent such information, and keeping in mind the impressive record of dissembling that NSA has so far amassed, it does seem to be a reasonable suspicion that the four cases discussed represent not a random selection from the list, but the best they could come up with. It that it so, the achievements of 215 do seem to be decidedly underwhelming.

In this regard, one could also examine that set of case studies of the 53 post-9/11 plots that have come to light by Islamist terrorists to damage targets in the United States.[97] Since these have resulted in public arrests and trials, there is quite a bit of information available about them. Overall, where the plots have been disrupted, the task was accomplished by ordinary policing methods. The NSA programs do not seem to come up at all.

---

[95] John Mueller, "Mueller on the Zazi Case: 'This is It?'" Informed Comment, juancole.com, November 4, 2009.

[96] *Hearing of the House Permanent Select Committee on Intelligence.*

[97] Mueller, *Terrorism Since 9/11*.

At the June 2013 hearings, one committee member, Representative Jim Himes of Connecticut, noting that his constituents were mainly concerned about 215, tried to get Alexander and Joyce to indicate how many plots would have been carried out but for that program: "How essential, not just contributing to, but how essential are these authorities to stopping which terrorist attacks?" Alexander irrelevantly responded that 702 contributed to 90 percent of the cases, and in half of these it was "critical." Further pressed about 215, the issue at hand, he said that "just over 10 of the cases had a "domestic nexus" and therefore 215 would apply, and that 215 "had a contribution" to the "vast majority" of these. Joyce then added more verbiage, proclaiming that every tool in the kit was both "essential" and "vital": "I think you ask an almost impossible question to say how important each dot was….Our mission is to stop terrorism, to prevent it….And I can tell you, every tool is essential and vital. And the tools [under discussion] have been valuable to stopping some of those plots. You ask, how can you put a value on an American life? And I can tell you, it's priceless."[98] Himes, out of time, ended by expressing his "hope" that "you'll elucidate for us specifically case by case how many stopped terrorist attacks" the 215 program was "essential to."

**Abandoning 215**

It certainly appears, then, that any benefit of the 215 program is considerably outweighed by its cost even assuming that the unknown, and perhaps unknowable, cost figure is quite small. That is, the program would very likely fail a full cost-benefit analysis handily even without taking into consideration privacy and civil liberties concerns. Representative Adam Schiff has done his own "on net" assessment. Even if the program is "occasionally successful," he

---

[98] *Hearing of the House Permanent Select Committee on Intelligence.*

concludes, “there’s still no justification that I can see for obtaining that amount of data in the first place.”[99]

In the past, NSA has actually closed down such programs—though not without characteristic dissembling. That is, it was persuaded to conclude that some tools in its kit were not necessarily all that “essential and vital.” James Bamford reports that the agency had a nationwide program to store e-mail and Internet metadata in bulk for years. It was ended in 2011 for “operational and resource reasons,” according to the director of national intelligence. But, notes Bamford, a statement issued in 2013 by senators Ron Wyden and Mark Udall contends that:

> the real reason the program was shut down was that the NSA was “unable” to prove the usefulness of the operation. “We were very concerned about this program’s impact on Americans’ civil liberties and privacy rights,” they said, “and we spent a significant portion of 2011 pressing intelligence officials to provide evidence of its effectiveness. They were unable to do so, and the program was shut down that year.” The senators added, “It is also important to note that intelligence agencies made statements to both Congress and the [FISA court] that significantly exaggerated this program’s effectiveness. This experience demonstrates to us that intelligence agencies’ assessment of the usefulness of particular collection program—even significant ones—are not always accurate.”[100]

It seems likely that, “on net” (as the President puts it) the highly-controversial 215 program could also safely be retired for “operational and resource reasons” with little or no negative security consequences. In 2002, risk analyst Howard Kunreuther proposed that a key question in evaluating terrorism security measures should be “How much should we be willing to

---

[99] Nakashima, “NSA cites case.”

[100] Bamford, “They Know Much More Than You Think.”

pay for a small reduction in probabilities that are already extremely low?"[101] If the 215 program has done little (and probably nothing) special to prevent or disrupt terrorist attacks in the United States, and if we are now having a healthy debate about the NSA programs, it seems reasonable to suggest that, even without full information about how the program costs, we are paying too much.

And, just possibly, there are other elements in the vast intelligence and policing empire spawned in panic and in unseemly haste after 9/11 that might also be retired.

---

[101] Howard Kunreuther, "Risk Analysis and Risk Management in an Uncertain World," *Risk Analysis*, 22(4) 2002: 662–63. See also John Mueller, "Some Reflections on What, If Anything, 'Are We Safer?' Might Mean," cato-unbound, September 11, 2006.

Preliminary Draft – Please Do Not Cite Without Permission
To be Published in *I/S: A Journal of Law and Policy for the Information Society*
9 ISJLP ___ (2014).
http://www.is-journal.org

# NSA Surveillance: The Implications for Civil Liberties

Shayana Kadidal[1]

What are the implications for civil liberties of the massive surveillance programs that have come to public attention as a result of Edward Snowden's disclosures? The first challenge for anyone attempting to unravel this issue is the natural tendency of the public to shrug[2] at the volume and complexity of the information flooding out -- from both Snowden and other, official sources that have started to speak to the media under the cover of his disclosures. The stories are rapidly evolving, and frankly complex enough to confuse anyone. But in my view the greatest contributor to the apparent complexity is the maze of ever-shifting, always highly technical *legal* justifications for the various programs at issue. In what follows, I will argue that the actual surveillance taking place is remarkably consistent from the Bush administration to the present day; although the legal rationales for the surveillance programs are protean, the programs themselves – and therefore their implications for civil liberties – are largely consistent. It is therefore both more enlightening (and simpler) to start a few years in the past, when most of us first heard about the NSA, in late 2005 when James Risen and Eric Lichtblau of the *New York Times* broke the story[3] that the NSA was collecting large quantities of calls and emails without getting approval from a court first, as usually happens with a conventional wiretap warrant.

## 21st Century Surveillance: A Brief History

[1] Senior Managing Attorney, Center for Constitutional Rights, New York City; J.D., Yale, 1994. The views expressed herein are not those of the author's employer, nor, if later proven incorrect, of the author.

[2] In internet terms, "TL;DR."

[3] James Risen & Eric Lichtblau, *Bush Lets US Spy on Callers without Courts*, N.Y. Times (Dec. 16, 2005), available at http://www.nytimes.com/2005/12/16/politics/16program.html?pagewanted=all

After holding the story for more than a year – past the 2004 presidential election – the *Times* finally published it in December 2005, shortly before Risen's book *State of War* (which included a chapter on the program) was scheduled for publication. Being the product of such a lengthy period of reporting, the story was rich in detail, but the main revelation was that the NSA, with presidential approval, has since shortly after 9/11 been intercepting calls and emails where one communicant was inside the U.S. and one abroad, where it believed that one of the parties was somehow affiliated with terrorism, all without any warrants or degree of judicial review whatsoever. The story was reported as an example of blatant lawlessness, for this "NSA Program" (as I'll call it throughout) appeared to circumvent the post-Watergate Foreign Intelligence Surveillance Act (FISA) statute that was designed to subject most foreign intelligence wiretapping to a system of judicial review similar to that that had applied to domestic wiretaps for criminal investigatory purposes since the 1968 Wiretap Act (or "Title III"). Indeed, the Bush Administration, which chose to aggressively defend the Program in the media, admitted as much: surveillance under the Program was of the sort that ordinarily would have been subject to FISA.[4]

That 1978 FISA statute, by appearances, was quite permissive: If the government could provide to the specialized Foreign Intelligence Surveillance Court (the FISC) evidence creating probable cause to suspect that a target was working for a foreign power (defined to include terrorist groups), it could get a FISA order – essentially, a wiretap warrant – allowing surveillance of that target's communications. In practice as well as in theory it seemed easy enough for the government to use: There were only five outright rejections among the first

[4] [CITE our SJ briefs; Gonzales press conference; note if space permits the argument that it might not have been "foreign surveillance" if intercepts were not in the US, but see Klein disclosures below.]

19000+ applications after 1978.[5] Though the administration would argue that judicial approval stood in the way of "speed and agility" in tracking down targets,[6] like Title III the original 1978 FISA provided for retroactive judicial approval in the event of emergencies. And in any event, the administration never asked a rather pliant Congress for approval of changes to the FISA statute, instead proceeding by executive fiat.

The political shockwaves the story generated were largely a consequence of this gross illegality; indeed the administration's spin seemed to project pride in its willingness to break the law, which added to the unease in my own community of civil libertarian litigators. Why not use FISA if the statute was that easy to work with? Our main suspicion at the time was that the administration was trying to eavesdrop on communications that even a very complaint FISC judge wouldn't approve of intercepting: conversations between lawyers and their clients, journalists and their sources. The description of the program – international calls and emails, with one end in the U.S., where one party was suspected (by an NSA staffer, not necessarily based on any tangible evidence) of association with terrorism – fit a vast quantity of our legally-privileged communications. The Center's legal staff frequently calls or emails released Guantanamo detainees, or their families, or witnesses relevant to their cases, or other overseas lawyers and experts. We also represented torture rendition victim Maher Arar, who lived in Canada at the time of the disclosures, having been released after a year of torture in Syria at the behest of our government, and representatives of a class of immigration detainees unfairly labeled as of interest to the 9/11 investigation, subject to over-long detention under brutal conditions, and subsequently deported overseas. They were all potential targets of the program, and though we need to communicate with them, we felt we had to take costly and burdensome

[5] [CITE in June 2006 MTD briefs] Roughly 1% of the applications were modified to some extent.
[6] [CITE Feb 2006 SOTU speech]

countermeasures (such as traveling overseas to meet in person rather than using the phone) given the existence of this judicially-unsupervised program of surveillance (which by definition did not operate under any judicially-supervised minimization procedures that might otherwise protect plaintiffs' legally privileged communications[7]). We felt the costs created by those counter-measures, the concrete manifestations of the chilling effect cast by the NSA Program, were sufficient to create injury-in-fact for standing purposes, so CCR brought suit seeking to enjoin the Program; the ACLU brought a similar suit (on behalf of itself, other lawyers, and journalists) on the same day in January 2006.

However, there were clues even then that this targeted NSA Program was only one aspect of the NSA's expanded post-9/11 surveillance activities. Risen and Lichtblau's initial story – and later others – reported, based on inside NSA sources, that there was a "data mining" component to the program – meaning, essentially, that the NSA was intercepting electronic communications (calls and emails) in a general fashion, not a targeted one, and then either scanning the content of those communications for the presence of certain keywords thought to be themselves suspicious, or applying more complex algorithms to that huge database to flag communications or the parties thereto for further scrutiny. To use a simple example of the latter, suppose a call comes in to a U.S. number from Afghanistan in the middle of the night, and the person called then then calls five other people within an hour. A mechanical algorithm can easily identify such situations (even where there was no prior reason to suspect any of the persons on the calls) and flag them for further review. The pattern the algorithm identifies may be characteristic of sleeper cells triggered to action; it may also be characteristic of a family wedding announcement being passed along to close relatives.

---

[7] [INSERT infra section below reference]

Within short order, a case was filed seeking damages against AT&T based on what appeared to be its complicity in just such a massive data-mining operation against its own customers. An AT&T employee whistleblower, Mark Klein, had disclosed to attorneys at the Electronic Frontier Foundation the existence of a secret room in AT&T's Folsom St., San Francisco switching station. It appeared that a copy of every electronic communication coming in off the fiberoptic undersea cables that entered AT&T's domestic system thru the Folsom St. station was being sent off to the NSA thru the equipment installed in the secret room; the only people who would enter the room were NSA staffers (who Klein frequently encountered lost, asking for directions, in the hallways) and one AT&T employee who held the highest security clearance. The complaint in EFF's case, *Hepting v. AT&T*, also alleged that AT&T had turned over its vast call records database to the government too – something which *USA Today* first reported was true of all three U.S.-owned telecom companies in May 2006.

In CCR's case and the ACLU case, the government challenged our standing, essentially asserting that if we had no evidence that we (or our other plaintiffs) were actually surveilled**,** our claims that we changed the way we use the phone and email because of the NSA Program's chilling effect were legally insufficient to support standing. But one group actually did have proof that they were surveilled. Al Haramain, an Oregon branch of an international Muslim charity, had been placed on the list of "Specially Designated Global Terrorist[s]" "due to the organization's alleged ties to Al Qaeda. ... [D]uring Al-Haramain's civil designation proceeding," Treasury officials inadvertently turned over to the organization's counsel a document labeled "top secret." "[A]fter *The New York Times*' story broke in December 2005, [Al-Haramain] realized that the … [d]ocument was proof that it had been subjected to

warrantless surveillance in March and April of 2004."[8] Published accounts state that this document provided evidence that the NSA had intercepted communications between an official of Al-Haramain and the charity's American lawyers, Wendell Belew and Asim Ghafoor,[9] whose practices are located in the Washington D.C. area—the sort of surveillance retention of which would surely never be approved of by a federal judge supervising a wiretapping order under the original FISA statute or Title III (absent an active role in some criminal conspiracy by the attorneys on the line), exactly the sort of communications we feared the NSA might have been targeting given its circumvention of the permissive FISA statute. This was not the only evidence supporting fears that attorneys' privileged communications were subject to warrantless surveillance: the Bush administration acknowledged in a formal 2007 submission to Congress that, "[a]lthough the [NSA] program does not specifically target the communications of attorneys or physicians, calls involving such persons would not be categorically excluded from interception."[10] And in 2008 the *New York Times* reported "[t]he Justice Department does not deny that the government has monitored phone calls and e-mail exchanges between lawyers and their clients as part of its terrorism investigations in the United States and overseas," and the *Times* further reported that "[t]wo senior Justice Department officials" admitted that "they knew of … a handful of terrorism cases … in which the government might have monitored lawyer-client conversations.[11] In CCR's own litigation challenging the NSA program, the government conceded before the district court that it would be a "reasonable inference" to conclude from

---

8 *Al-Haramain Islamic Foundation, Inc. v. Bush*, 507 F.3d 1190, 1194-95 (9th Cir. 2007).

9 *See* Patrick Radden Keefe, State Secrets: A Government Misstep in a Wiretapping Case, The New Yorker (Apr. 28, 2008); Jon B. Eisenberg, Suing George W. Bush: A bizarre and troubling tale, Salon.com (Jul. 9, 2008).

10 Assistant Attorney General William E. Moschella, Responses to Joint Questions from House Judiciary Committee Minority Members (Mar. 24, 2006) at 15, ¶45, *available at* http://www.fas.org/irp/agency/doj/fisa/doj032406.pdf (last visited Sep. 20, 2012).

11 Philip Shenon, *Lawyers Fear Monitoring in Cases on Terrorism*, N.Y. Times (Apr. 28, 2008), at A14.

these statements of government officials "that some attorney- client communications may have been surveilled under" the Program.[12]

Two months after we sued, Al-Haramain and the two U.S. attorneys sued seeking damages. After years of litigation, the Ninth Circuit found the document protected by the state secrets privilege: notwithstanding its accidental and seemingly negligent disclosure, it was still classified top secret, still a state secret, and thus couldn't be used in litigation. Put to one side the original copy of the document, now filed with the court—even the attorneys' memories of the document couldn't be referred to; the proof of surveillance missing from our case was here secret and thus entirely unavailable to the Plaintiffs.[13] After further proceedings, the lower court nonetheless found that plaintiffs had established a prima facie case of unlawful surveillance based on circumstantial evidence effectively uncontested by the government, and awarded damages and attorneys' fees, but that ruling was overturned on sovereign immunity grounds by the Ninth Circuit.[14] The case EFF filed against AT&T sought damages, and it died when congress passed a retroactive immunity statute, though otherwise they might well have ended up with the same problem as *Al Haramain* given the whistleblower documents' centrality to the claims.

As to our cases, seeking to enjoin the program, the government very aggressively defended the program in public and in court, but then shifted tactics by convincing a FISC judge to approve the whole program by January 2007, just in time to abort the first court of appeals argument challenge in the ACLU case. Different FISC judges reviewed the initial January 2007 order or orders and rejected what the first more pliant judge had approved of;[15] that, in turn,

---

12 *See* Defs. Reply Br., Dkt. 49, *CCR v. Bush*, No. 07-1115 (N.D. Cal.) at 4.

13 *Al Haramain*, *supra* note ***.

14 *Al-Haramain*, 2012 U.S. App. LEXIS 16379 (9th Cir. Aug. 7, 2012).

15 [CITE stories – pull from sup brief August 2007]

finally provoked the Bush Administration to seek approval from Congress for the NSA's program of surveillance without individualized judicial review of targeting decisions. That approval came first in the form of a temporary statute, allowing the government to seek broad approval for whole programs of surveillance (without individualized review of targets) from the FISC for a six-month period. That authority expired in early 2008, with the presidential campaigns well underway.

Eventually in 2008 the Bush Administration gained lasting Congressional approval to change the post-Watergate-era FISA statute beyond recognition, so that the government would propose a whole program of surveillance to one FISC judge, who would then check off on the whole thing if it seemed designed to sweep in primarily foreign communications. Essentially this was a codification of the existing NSA Program with a veneer of judicial review. [ADD: detail on why FAA jud rev is insubstantial***] When Senator (and presidential candidate) Obama switched his position and voted in favor of that statute, the 2008 FISA Amendments Act (FAA), he effectively removed surveillance from the public political debate for the next five years, because it was no longer a bone of contention between the parties.

The ACLU challenged the FAA in court an hour after it was signed into law, claiming primarily that it violated the Fourth Amendment, and that case, *Clapper v. Amnesty International*, went to the Supreme Court on the same standing issue that the government had made its primary defense to the 2006 cases brought by CCR and the ACLU against the NSA Program. In a 5-4 decision, the ACLU lost: the Court didn't quite say that you need absolute proof that you were surveilled, but it said our chilling effect theory wasn't valid at least where the FISA court was reviewing things for compliance with the statute and the Fourth Amendment,

as the statute mandated. (The remnants of our original 2006 case, now in the Ninth Circuit on the issue of records retention by the government, were dismissed as well, relying on *Clapper*.)

For future litigants resembling the CCR and ACLU plaintiffs, this first round of NSA litigation set up a framework for any future litigation that is essentially a Catch-22: where plaintiffs lack direct evidence that they were surveillance targets (that is, where reasonable measures taken in response to reasonable fears of very broad surveillance are the only basis for a civil litigant's injury), they are likely to be tossed out of court on standing grounds based on *Clapper*. Where plaintiffs do, somehow, have direct evidence of past or present surveillance, and try to bring a civil suit for damages or try to enjoin interception or retention of records under the surveillance program and have it declared illegal, the evidence of surveillance will be tossed out of court as secret.

Of course – as the majority noted in *Clapper* –this leaves the possibility that the government will seek to introduce evidence from such surveillance in a criminal case, and the defendant will then be able to litigate the validity of the surveillance under the Fourth Amendment regardless of the statutory basis *vel non* of the surveillance. In fact Solicitor General Verilli specifically argued to the Court that federal courts didn't need to reach the merits of the ACLU challenge precisely because the same issue would eventually come up in some criminal case. Of course, that assumes the government wants the issue to be litigated; a typical (strong) criminal case will rely on many veins of evidence, not all of which may be fruits of initial NSA surveillance, and if so, the government may choose its evidence to avoid bringing NSA evidence into court. It is unclear that any previous criminal case has challenged actual surveillance under the NSA Program or any of the other programs reported on since the Risen/Lichtblau story, leading us to one of two conclusions: either all the litigation over the validity of such broad

surveillance has been done in secret, with the parties lodging all arguments *in camera*, or that the government has failed to acknowledge that evidence that did in fact derive from NSA surveillance was the fruit of the same. It appears, based on recent reports, that the latter is in fact the case: that the Justice Department's policy was not to acknowledge to defendants the origins of evidence that was the fruit of surveillance under the current mass surveillance programs, that it changed position in response to pressure from the Solicitor General, and that a first such acknowledgment occurred on October 25, 2013.[16]

In any event, absent the odd criminal case that is entirely reliant on evidence gathered by NSA, such litigation will proceed only when the government desires it to. The same could be said about other cases involving proof of actual surveillance, such as *Al-Haramain*: if the government wanted to litigate the legality of NSA Program surveillance of American attorneys, it had the option to not assert the state secrets privilege there. In the current round of Snowden-inspired litigation, the government has acknowledged the authenticity of the Section 215 order allowing for mass gathering of calling records, enabling the ACLU's litigation over that program to go forward on the merits. Though this was likely necessary to justify the government's release of a second order apparently limiting use of the records database, it perhaps is a sign that the government (a) believes it will win and (b) feels that it needs the political cover of a favorable ruling on the legality of the call records program from a non-FISC judge.

**From Risen/Lichtblau to Snowden: Current-day programs**

[16] Charlie Savage, *Federal Prosecutors, in a Policy Shift, Cite Warrantless Wiretaps as Evidence*, N.Y. Times (Oct. 26, 2013), available at http://www.nytimes.com/2013/10/27/us/federal-prosecutors-in-a-policy-shift-cite-warrantless-wiretaps-as-evidence.html?nl=todaysheadlines&emc=edit_th_20131027&_r=0

Even this short history of NSA surveillance from 9/11 thru early 2013, told thru the litigation narrative, shows a pattern: similar programs run under legal authority that shifts so dramatically that the legal justification for the surveillance eventually comes to seem an afterthought, rather irrelevant to the (typically unbounded) shape of the surveillance program itself.

So, initially after 9/11, the NSA's various warrantless surveillance programs (some aimed at the content of communications like the NSA program we challenged in our 2006 suit; others aimed at metadata like the phone records program described in *Hepting*) operated under nothing more than the authority of the president's say-so, backed by a single Office of Legal Counsel memorandum as cover. That memo was shielded from the OLC's usual oversight processes by disingenuous use of security clearances to hide it from scrutiny. By 2004, we now know that Jack Goldsmith and James Comey forced some aspects of those programs to stop, so the administration turned to National Security Letters to run its metadata programs and changed others.[17] When the Risen/Lichtblau story revealed some of the warrantless electronic content surveillance programs, the administration first defended its executive legal prerogatives shamelessly; then, confronted with a Court of Appeals challenge, went to the FISC court for what turned out to be a few months of reprieve, and when forced by the FISC's change of heart, finally went to Congress to broaden the statute, first in temporary sunsetting fashion, and then more permanently with the FAA. As Marcy Wheeler summarizes it: "As the authorities [for] one program got shut down by exposure or court rulings or internal dissent, [the surveillance] would migrate to another program."[18]

---

[17] [CITE Benkler p2]

[18] [CITE Marcy's piece:] http://emptywheel.firedoglake.com/2009/10/07/bushs-illlegal-domestic-surveillance-program-and-section-215/

In light of this pattern, it's probably not surprising that today the stories speak not of one "NSA Program" but of a "crazy quilt"[19] of code names: "PRISM," "BLARNEY," "Transient Thurible," the palindromically-menacing "EvilOlive," "Shell Trumpet," "Spinnaret," "Moon Light Path" and so forth. NSA whistleblower Thomas Drake explains the profusion of such names by analogy to the perceived need to come up with catchy company names and job titles within startup/dot-com corporate culture, or "app" names for the iPhone generation. In part because discussions structured around particular programs as marketed within NSA are meaningless to what's going on, and in part because the confusion engendered by all the flashy code names makes people tune out, I want to simplify by classing things into two main sets of programs: those that collected the content of communications, and those that collected non-content information about communications, the latter generically referred to as "metadata" – roughly the letter and the envelope, to use the most evocative metaphor.

***Metadata Surveillance***

The most publicized of the NSA's metadata programs was one through which the agency, under section 215 of the Patriot Act, got a series of court orders, repeatedly renewed over the years going back to 2006, allowing it to collect all phone records from Verizon Business (and likely the two other domestically-owned ["controlled"? What is the precise term here?] phone providers as well[20]). So the NSA requested and received from these telecom companies lists of all calls their subscribers made and received, including typically-recorded metadata such as the

[19] [CITE to paraphrase the dumbest line in *Smith v Maryland*]
[20] [CITE]

time of day, duration of the call, and of course the phone numbers on the other end of the line (but not the content, i.e. what was said on the call.)

The order published by the *Guardian* newspaper could easily be read standing alone to simply demand that these records be turned over to the NSA for whatever use it chose to make of it. The administration subsequently released other orders that indicated that the FISC orders only permitted it to query the database of calling records so assembled to investigate records of someone's calling patterns when "a small circle of designated NSA officers" felt they had "reasonable articulable suspicion" that that person had some connection to terrorism,[21] but it also admitted that it then scrutinized the calling records of everyone that first person called, and everyone those people called. On Frigyes Karinthy/Six-Degrees-of-Kevin-Bacon principles, that surely includes a huge swath of humanity for each of the 300 individuals[22] the NSA has allegedly limited its phone database investigations to; depending on input variables about the size of the typical acquaintance pool, estimates have varied between 3 million and tens of millions of people per target. Other metadata collection programs have been disclosed since then, including a series of programs to collect all web surfing data (that is, all internet addresses a consumer visits), under the not-at-all menacing name EvilOlive. A firm picture of how many steps out from an initial suspect the NSA will reach is not clear for other metadata programs.[23]

The administration's defenses of the call records program as policy have focused on both the limitations on querying the database referred to above, and the idea that this information is the same data that the private telecom companies already keep on their subscribers, as they routinely track usage for billing purposes, the main differences being duration of retention (the

---

[21] Steven G. Bradbury, *Understanding the NSA Programs*, 1:3 Lawfare Res. Pap. Ser. 1 (Sep. 1, 2013).

[22] [CITE]

[23] *See, e.g.*, Shane Harris, *Three Degrees of Separation is Enough to Have You Watched by the NSA*, Foreign Policy (Jul. 17, 2013), available at http://killerapps.foreignpolicy.com/posts/2013/07/17/3_degrees_of_separation_is_enough_to_have_you_watched_by_the_nsa (three steps, citing testimony of NSA Dep. Dir. Chris Inglis).

FCC requires no more than 18 months; the NSA claims it keeps these records no longer than five years) and the fact that many companies' data are now accumulated into one NSA database, allowing for a more complete picture of the interrelationships between callers who subscribe to different providers.

In some ways this defense points us towards the root of the real problem for civil liberties. Private companies routinely accumulate huge volumes of data about we consumers in order to sell us more product: not just the usual corporate suspects like Google (who can discern which banner ads are likely to get your attention for an advertiser -- and be useful to you – by scanning thru your email to tell what things are occupying your thoughts), but also your supermarket or drug store. Those free loyalty cards that Duane Reade urges consumers to sign up for are used to track a consumer's identity and create a purchase history tied to that identity. The frequent sizeable discounts given to cardholders on many goods are worth the bargain for the merchant, who can then start targeting those consumers with customized ads and discount offers to draw them back into the store.

Interestingly, the NSA, with access to many more streams of data, may have been doing this on its own by pulling together many consumer-purchase databases[24] with credit card records. The most prominent example of a case NSA claims its newly-revealed operations helped uncover, would-be New York City subway bomber Najibullah Zazi, was said to be making TATP (acetone peroxide) bombs with cosmetic peroxide. Early in the investigation the FBI cited to three other individuals near Zazi's Colorado town who also bought small quantities of acetone

[24] It has frequently been noted that many consumer profiles available from companies that specialize in assembling them are underwhelming in how accurate a picture of an individual's preferences they assemble, *see, e.g.*, Paul Rosenzweig, *How to Find Out What big Data Knows About You*, New Republic (Oct. 7, 2013); again, along the lines of any network effect, the combination of several sources should be expected to exponentially increase the usefulness/intrusiveness of a profile.

or peroxide; they were never mentioned by officials again,[25] but the fact the FBI could identify presumably innocent individuals as suspects so quickly is a clue that perhaps the government has assembled a massive database of consumer purchasing records by agglomerating a large number of similar databases collected by companies. As with the phone records database, expanding the databases expands the number of hits one may generate for a narrow query (e.g. people who purchased peroxide in X quantity within Y miles of Aurora, Colorado; people who are two call steps removed from a terrorist's cell phone).

But the fact that three innocent Coloradoans may have been briefly flagged as of interest to a real terrorism investigation by dint of benign consumer purchases is not the problem here – alarming as it may be to average Americans who felt they had "nothing to fear" from NSA activities. Nor are the potential flaws with the government's (or the court's) interpretation of the scope of which records may be the subject of a Section 215 order. While the government's reading of Section 215 of the Patriot Act – one that the largely conservative judges of the FISC have agreed with – is a broad one, and perhaps had a distorting effect on annual reporting to Congress of the number of times Section 215 had been used, the question of Congressional intent is one on which reasonable people can disagree.[26]

The true legal problem underlying broad metadata collection programs is that the government has long believed it doesn't need a court order of any kind to grab information like these phone records, because the Fourth Amendment doesn't even apply to them under what's called the "third party doctrine." In *Smith v. Maryland*, 442 U.S. 735 (1979),[27] the Supreme

---

[25] Marcy Wheeler, *Meet 3 PATRIOT Act False Positives Investigated for Buying Beauty Supplies* (Jun. 7, 2013) available at http://www.emptywheel.net/2013/06/07/meet-3-patriot-act-false-positives-investigated-for-buying-beauty-supplies/#sthash.77GH0OHW.dpuf

[26] [CITE flaws with statutory interp of 215: my MSNBC notes; Mike Germain's piece; Kerr's Volokh piece on the Eagan opinion; contra: Bradbury Lawfare paper]

[27] [note, per Kerr, that Miller (banking records) preceded Smith?]

Court held that government doesn't need a warrant to track the phone numbers you call because you are handing those numbers over to the phone company to route your call (and bill you for the service) every time you dial a number, and once you *voluntarily* give any information to a third party, the government is entitled to simply demand it from the third party as readily as if it were a confession you'd given to your neighbor.

So the fourth amendment and its warrant protections don't apply to information like dialed phone numbers – that you turn over to a third party for their use. The most frequent analogy used to justify the distinction between the private contents of the phone conversation (protected by the Fourth Amendment) and the numbers (not protected) is the difference between the address written on the outside of a letter and the contents of the envelope: the contents are protected, the address is not. [28]

*Smith* is widely criticized; one reason most people haven't heard about it is that Congress re-regulated much of this area by statute shortly afterwards, in response to the decision. The Court said it was "doubtful that there is a reasonable expectation of privacy" in the numbers, perhaps because that was an era of being billed per call, but at the time local numbers didn't show up on most bills, a fact to which the Court has no answer beyond saying it was "not inclined to make a crazy-quilt of the fourth amendment" by making its rule turn on the distinction between local and long-distance numbers. Commentators have also suggested the case should simply be confined to its facts and understood as an implicit consent case (something Marshall's dissent refutes by pointing out the illusory nature of consent in the context of monopoly providers of telecom services). In the modern era of unlimited (or volume) calling

[28] We now know, coincidentally, that the Post Office is scanning the outside of all mail envelopes in its system for the government. *See* Ron Nixon, *U.S. Postal Servive logging All Mail for Law Enforcement*, N.Y. Times (Jul. 3, 2013) (describing the "Mail Isolation Control and Tracking" program, instituted after post-9/11 anthrax mail attacks).

plans one might readily questions whether the crazy-quilt is simply the content/routing information distinction: why shouldn't the content of the phone call also considered something "voluntarily turned over to the phone company"? And it is hard to square the notion that people lack an expectation of privacy in their electronic communications records nowadays, where the degree to which we live our lives online would have been unimaginable in 1979.

The government, however, believes the upshot of *Smith* is that vast categories of information we digital moderns usually assume will be kept private can in fact be obtained by the government without asking a court for approval. Instead, the government need only issue a subpoena to your corporate provider. So not just phone records (who you called and who called you), but records of internet web sites you visited,[29] all your banking records and credit information, records held by your travel agents, older emails stored by your email provider, and drafts of emails, and files you store on the cloud, all can be obtained without court order through issuance of a subpoena to the corporate third party holding the records or other material on behalf of you, the consumer. That is shockingly broad list, including essentially all of your commercial interactions with the outside world.

There are very limited restrictions in the caselaw on what the government can subpoena,[30] and Congress has passed statutes authorizing broader subpoenas – National Security Letters are the variant most widely known to the public —allowing various sorts of business records to be demanded *en masse* without judicial involvement.[31]

Professor Barnett claims there are legal safeguards with more teeth available to providers than to consumers seeking to challenge overbroad subpoenas, "if the provider doesn't want to

---

[29] [CITE judicial decisions on Internet data from Kerr?]

[30] [only right under subpoena: must not be overly burdensome *to comply with* (Kerr 7: "sufficiently limited in scope, relevant in purpose, and specific in directive so that compliance will not be unnecessarily burdensome")

[31] [CITE Dycus 649, 639 for the lists and charts; perhaps also Kerr's chart]

turn over the records."[32] But the providers of most concern here are telecom companies. And the telecom industry is so heavily regulated -- and so beholden to government on rate regulation, taxes, antitrust issues, wireless bandwidth access -- that it has every reason to cooperate with any demand, no matter how legally outrageous. Its track record over the last decade is proof in point: only Qwest offered any resistance to the NSA Program, there appears to have been no provider resistance to the Section 2i5 phone records collection program, and the instances of even internet companies (arising out of the famously libertarian culture of Silicon Valley) fighting back against third party subpoena requests are rare enough to make news when they happen. Only several months into the Snowden stories – as worries about defection of foreign customers to non-U.S. providers have perhaps mounted – do we read frequently about outrage at companies with an international consumer market such as Google and Yahoo.[33]

So the debate over enhancing FISC review – in terms of general transparency, adversary process (by appointing a sort of Devil's Advocate to argue *in camera* for the public's or targets' interests), and judicial selection reform and panel seating on that court,[34] should ring a bit hollow: the government doesn't need to go to the FISC to collect any of this metadata. It's just sometimes easier to use Section 215 than other authorities, and if the protean past of these programs is any clue, in the future the government may shift towards using various subpoena powers anyway.

One stream of metadata by itself can reveal a lot about you. Commentators have already exhaustively catalogued the obvious examples: the records of your calls to your therapist, to a divorce lawyer, to a drug rehab center, all can reveal things about you that you might rather keep secret, and taken together the sum of your communications metadata can form a picture of your

---

32 [CITE Barnett – Volokh]

33 [CITE Gellmann "smileyface" story -- Oct 30]

34 [CITA Bruce Ackerman LAT proposals for reform (the only ones that include the panel, AFAIK)]

inner life and your political beliefs that few of us would want to share with the government either.

Ironically, one particularly corrosive aspect of metadata surveillance that has been drowned out by the Snowden revelations was the previous surveillance scandal of the year, the seizure of the Associated Press' phone records. In an investigation of a leak at the center of a story worked on by seven reporters, the Justice Department authorized seizure of records from 20 lines in four offices used by 100 AP reporters. If the government can see that three government officials spoke to a reporter the day before a story revealing some embarrassing government secret is published, it will not be hard to piece together who the source is. For these most sensitive communications – reporters with sources, attorneys with clients -- fear of such metadata surveillance will case a massive chilling effect, just as surely as fear of the NSA Program's surveillance of the *content* of communications cast a chill on the communications and therefore on the litigation activity of the CCR and ACLU attorney-plaintiffs in the 2006 litigation.

Like this recent AP phone records seizure, past broad phone records seizures directed at reporters have seemed punitive in scope. Several years ago, John Solomon of AP was a target of a phone records subpoena, after he published a story about the FBI's botched investigation of corrupt New jersey Senator Robert Torricelli. Two years later Solomon spoke to a number of former sources who told him they stopped calling him because they knew he was a target.[35] The metadata seizures, in other words, had had a chilling effect on the willingness of *others* to use the phone to talk to him – in much the same way as various third parties were no longer willing to speak to the attorney-plaintiffs in the NSA program and FAA litigation.[36]

---

35 [CITE is in MSNBC notes]

36 [CITE Meeropol aff; ACLU 2006 aff; Clapper amicus – Kassem, Foster]

One might conclude that reporters in this area really need to work like Woodward and Bernstein in the parking garage, or like the drug dealers in *The Wire*: constantly buying and disposing of burners (cheap prepaid cell phones) to communicate. However, even that strategy is at risk given the breadth of the Snowden metadata revelations: it has been reported that one use of the massive phone records databases has been to use calling patterns to identify disposable phones with known targets by identifying their known calling networks and working backwards.[37]

Having several streams of data (not just calling records) can reveal a lot more: studies have shown that analyzing your friendship group can reliably predict whether you are gay or not.[38] A less-scientific analysis of social club memberships of 254 prominent Massachusetts colonials produced Paul Revere as the most centrally-networked figure of the bunch.[39] And it turns out NSA is getting a lot of different streams of data and attempting to assemble full "social graphs" (a term probably mostly familiar from Facebook's search-your-friends feature called Graph Search) for targets. But they are also doing it directly: in October it was reported that NSA is collecting millions of contact lists from email accounts – essentially, grabbing ready-made social network maps.[40]

One unknown area is the extent of NSA gathering of mobile phone location data. Does it fall in the same third-party category as the other records above?[41] The issue is as yet unresolved in the courts. Interestingly, the Supreme Court is clearly sensitive to the notion that government tracking of the movement of citizens may implicate Fourth Amendment interest. In *United States*

---

37 [CITE]

38 [CITE "me and my metadata"]

39 http://kieranhealy.org/blog/archives/2013/06/09/using-metadata-to-find-paul-revere/

40 http://www.washingtonpost.com/world/national-security/nsa-collects-millions-of-e-mail-address-books-globally/2013/10/14/8e58b5be-34f9-11e3-80c6-7e6dd8d22d8f_story.html (p.3: "no content present")

41 [Kerr article: summarizes litigation]

*v. Jones*, 132 S. Ct. 945 (2012), a case invalidating evidence derived from a GPS tracker physically installed on a suspect's car (and operated in excess of the narrow geographical and temporal scope allowed by warrant), the Court's opinion held Justice Alito's concurrence noted that "longer term GPS monitoring" implicated expectations of privacy, 132 S. Ct. at 964, and Justice Sotomayor's concurrence stated more broadly:

More fundamentally, it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties. … This approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks. People disclose the phone numbers that they dial or text to their cellular providers; the URLs that they visit and the e-mail addresses with which they correspond to their Internet service providers; and the books, groceries, and medications they purchase to online retailers. Perhaps … some people may find the "tradeoff" of privacy for convenience "worthwhile," or come to accept this "diminution of privacy" as "inevitable" … and perhaps not. I for one doubt that people would accept without complaint the warrantless disclosure to the Government of a list of every Web site they had visited in the last week, or month, or year. But whatever the societal expectations, they can attain constitutionally protected status only if our Fourth Amendment jurisprudence ceases to treat secrecy as a prerequisite for privacy. I would not assume that all information voluntarily disclosed to some member of the public for a limited purpose is, for that reason alone, disentitled to Fourth Amendment protection.

This may be the rare area that is promising for privacy advocates to bring before the court, as a number of recent Fourth Amendment cases have broken along unpredictable voting lines at the High Court – neither democrat-republican nor the other usual variant, pragmatist (Breyer, Roberts)-vs-formalists (Scalia, Ginsburg).[42]

***Content Surveillance***

I have very little to say about the details of the NSA's contemporary content surveillance programs, in part because they seem to be largely continuous with the NSA Program surveillance that we challenged in 2006, and that was intended to be effectively codified by the 2008 FAA statute that the government has said is the source of legal authority for the PRISM surveillance program.[43] PRISM was the subject of the second major Snowden-sourced story to appear, and was perhaps the received with the most outrage because it showed how closely the telecoms and internet companies were cooperating with the NSA.

Gen. Alexander has succinctly characterized these programs by stating that "our goal is to collect everything."[44] With PRISM it is collected from the servers of just about every consumer IT company one can think of: Google, Facebook, Apple, Microsoft, Youtube. Even Skype, which used 256 bit encryption to transmit video calls over the internet, was a party – as a consumer, the encryption ensured that your video call was safe even in international transit, but the company that you were trusting to encrypt it might well have been handing over your content data to the government under the FAA. (So Skype consumers like us, who are maximally

42 [CITE e.g. *Maryland v. King*; cases in Kerr at 4-5]
43 [CITE govt press statement on 702 surveillance]
44 [CITE]

paranoid about security, are vulnerable just as much as the internet primitives using AOL and Yahoo (which were also participants in PRISM).)

As for communications in transit, NSA programs such as BLARNEY intercept almost everything as it passes from major hub to major hub on the internet's backbone fiberoptic cables. This is exactly the sort of interception that Mark Klein reported was happening within AT&T switching stations in 2006. (Amazingly, this internet traffic can all be searched in real time by NSA analysts using NSA's XKeyscore data retrieval system.)

Because corporate providers typically store large troves of *metadata* (and have commercial incentives to hold on to it for some time and analyze it in some detail), the question of whether it is feasible for the government to seize and store the same is rarely asked. But when stories claim that massive *content* interception and storage is taking place, the public's first reactions always is: is that even technologically feasible? While the answer was uncertain to our technology experts in 2006, the answer today is clearly yes. In their 2011 book *Cypherpunks*, Julian Assange and Jacob Appelbaum conclude that it would cost around $30M to store all phone content in and out of Germany for a year. Even quadrupling that to adjust for the greater U.S. population is trivial in comparison to the NSA's $12B budget. (When East Germany still existed and was trying to achieve this level of surveillance, 100,000 members of the 16 million person population worked for the Stasi, which needed 10,000 staffers simply to transcribe wiretaps. Now an array of iPhones could accomplish the same.) The cost may be even less now, in 2013: Brewster Kahle estimates it would take under 300 Petabytes (300,000Tb) to hold all U.S. traffic for a year, and that the hardware required to store all that would cost about $20M. For years there have been stories that the NSA is building a massive storage center in Utah

capable of holding 12,000Pb of data.[45] As long as NSA can keep the power running to it (allegedly at a cost of $20M a year), they have more than the capacity they need. So when an FBI agent on CNN claims the government will be able to go back and listen to calls Tamerlane Tsarnaev made to his wife *before* the Boston bombing, the claim may be realistic.

The main point to remember about these massive content dragnets is that this is precisely how civil libertarians were saying the 2008 surveillance amendments that Senator Obama signed off on a few months before the election would be implemented when the FAA passed. The ACLU filed *Clapper* an hour after President Bush signed the FAA, arguing that it had almost no practical limitations. The FAA allows content surveillance not based on any individual suspicion presented to the FISC. Instead, the court approves criteria for a whole program of surveillance, and reviews it only to see that the criteria seem intended to sweep in communications of people located outside the US. There seems to be next to no after-the-fact review provided for, although cases of the NSA misrepresenting the scope of collection practices seem to have been common based on several FISC opinions declassified (with the intent to reduce public criticism of that court's secretive process) in the wake of the Snowden revelations.

**Protections (and their failings)**

So that's what's happening factually. Even in simplified form it can be confusing and overwhelming, and that does mute the voting public's response. But we shouldn't extrapolate from that the public doesn't care (and, from that, that Congress will never care either). Public polling data is highly consistent on this front, and it has been since just after 9/11 to the present

[45] http://www.forbes.com/sites/kashmirhill/2013/07/24/blueprints-of-nsa-data-center-in-utah-suggest-its-storage-capacity-is-less-impressive-than-thought/

day: when the American public believes that surveillance is targeted at terrorists or targeted at foreigners, it doesn't mind that it is happening on a larger-than-expected scale. But the moment the public believes that surveillance – even not-very-deep surveillance like the non-content programs discussed above – has a chance to touch on *their* communications, a strong reaction follows. So the public's reaction to these programs is actually nuanced and stronger at times than many seasoned observers would anticipate.

Perhaps the best example of this in practice is the reaction to John Poindexter's Total Information Awareness (TIA) program – which aspired to conduct mass surveillance from various data streams and filter that mound of big data in revealing ways. When its existence came to light in 2003, the public was horrified.[46] (Though surely choosing a disgraced Iran-Contra figure as the program's leader didn't help, the fact that the program itself touched the communications of many ordinary Americans seemed to provoke most of the revulsion.) Congress felt the pressure from the voting public enough to (at least gesturally[47]) pull the funding for the program shortly after it became publicized.

Of course, for people like journalists and attorneys whose communications are especially vulnerable, all the serious chilling effects noted in *Clapper* and the 2006 lawsuits continue to exist in light of both the content and metadata programs that we know are continue (albeit under occasionally varying legal authority) today. Surely these chilling effects exist with members of the general public as well: just ask any recent college graduate whether they limit what they post on social media out of fear of what some future employer may find there, and extrapolate that to political associations that some future government may find criminally suspect – Palestinian activists, radical environmentalists, etc. [*Might think about moving these two graphs way down*

[46] [general CITES see 2006 TPs]
[47] [CITE some funding continued]

*to the concluding thoughts about Congress—but there may be references in text between here and the end that then need moving*.]

What, then, are the safeguards that concerned members of the public might look to? And do they really offer any comfort?

***Judicial review***

On the metadata front, there's been a lot of talk in the media about the failings of the FISC (especially after, later in the summer, a pretty poor opinion was released justifying the call records program written by a judge renewing the 215 order that was published in the *Guardian*). But again, the most important point to note is that the government believes, because of the third party doctrine, it doesn't even need court orders if it chooses to gather this material with subpoenas (and NSLs are really just a Congressionally-created type of very broad subpoena). When the government next shifts legal theories for its metadata collection, it won't matter what Congress' precise intent with Section 215 was.

It's also clear the FISC doesn't often get the information it needs. A number of its decisions were released in unclassified form after Snowden; previously there had not been any from the FISC itself, though a few opinions of its appellate court had been released. One 2009 decision said the government had "repeatedly submitted inaccurate descriptions" of the program the FISC was reviewing; two years later, a 2011 opinion noted the government had disclosed a "third instance in less than three years… [of] a substantial misrepresentation concerning the scope of a major collection program." But each time the NSA tinkered with its internal controls and procedures, and was allowed to keep going by the Court.

Of course the way the court hears matters – *ex parte*, like any court hearing warrant applications – is not conducive to rejecting many applications, and the composition of the court (with judges selected by Chief Justice Roberts, all of whom were appointed by republican presidents) and the government able to choose the first judge it approaches whenever a new form of surveillance is proposed (presumably a factor in the January 2007 order(s) that were quickly reversed on renewal review by other FISC judges), one would not expect it to produce much. [48] But my own impression is that many reform proposals circulating currently are merely "tinkering with the machinery of mass surveillance" (to paraphrase Harry Blackmun); the overbroad scope of the FAA statute[49] and the statutes governing third-party records requests (NSLs, Section 215 orders, and their like) is the true problem, and one that would go unaddressed even if the public interest had an *in camera* advocate, the judges sat in banks of three, were not hand-picked by the Chief Justice, and the court enjoyed more transparency than exists now. Moreover, most metadata collection lies entirely outside of FISC review—for example, the email address-book collection program revealed In mid-October occurs outside the U.S. and so is only subject to the NSA's internal "checks and balances."[50]

Finally, the traditional model of judicial review loses all meaning when it's applied to mass surveillance *programs*. If extending the physical search warrant to wiretapping posed the difficult conceptual problems presaged in *Berger*, the Title III individualized-suspicion model of judicial review seems completely incompatible with mass surveillance. Particularity is at the center of judicial review of warrant applications; there is no equivalent when a court is asked to

---

48 [CITE Benkler;Wheeler blogs]

49 Interestingly, in denying standing in *Clapper*, the Court assumed the robustness of FISC review. The Court cited five factors that ought to have given the plaintiffs some comfort, most notably of which was the fact that, under the statute, the FISC was supposed to review FAA content-collection applications to ensure compliance with the 4th Amendment. So the weakness of FISA Court review would seem to make the chilling effect felt by plaintiffs there more reasonable.

50 [CITE]

review a proposed program of surveillance, a set of criteria for targeting. It's a bit like applying strict scrutiny's narrow tailoring test to the compelling interest of diversity. The ACLU was correct to portray the FISC's review of FAA applications as absurdly shallow in *Clapper*, especially in light of the apparent absence of any strong judicial oversight of the minimization procedures meant to ensure that domestic conversations (and, as we wrongly assumed, *infra* part ***, privileged conversations) were in fact being filtered out notwithstanding that they might have met the broad criteria for information gathering under the proposed programs. This has led many commentators to assume that any review of such broad programs will turn on the first half of the Fourth Amendment – on "reasonableness," standing alone – ignoring the second half (the particularity requirement for issuance of warrants, which the modern court has generally grafted onto the first half in holding warrantless searches per se unreasonable).

***Congressional oversight***

The well-catalogued duplicity of NSA officials has certainly contributed something to Congress' failure to limit the agency's activities over the years. Put to one side glaring examples such as DNI James Clapper's response to Sen. Wyden's question "Does the NSA collect any type of data at all on millions or hundreds of millions of Americans?" – "Not wittingly" – which Clapper later characterized as the "least untruthful" answer he could in open session.[51]

But an underreported aspect of the problem is the fact that by constantly shifting the *legal authority* used to conduct substantively-consistent mass content and metadata surveillance, the

[51] Of course, Wyden had let him know the questions in advance, so the idea that Clapper had to lie on his feet to protect classified information defies credulity; his own defense, in fact, was that "collect" means something technical to a surveillance junkie like himself, and so he was simply confused by what otherwise seemed like a straightforward question. [CITE *See also 9 Big Lies* post]

agency presents an always-shifting target for Congressional oversight. So by the time a hidden OLC opinion comes to light, the mass content surveillance is being conducted under FISC order. Hearings about one form of NSL usage bog down in details and repeated, time-consuming requests for better data; by the next year, the same records may be being gathered via a 215 order.

The high classification levels of these programs (and Congressional deference to such designations) have also negatively impacted oversight. The NSA Program was, notoriously, described in top secret briefings to the members of the intelligence committees, including many democrats. But they were not allowed to bring their legal staffers into those briefings due to classification/need-to-know concerns asserted by the administration. Jay Rockefeller went as far as to protest this in a (classified) letter (that itself was allowed to be released only after the program was disclosed by the *Times*) to the administration, noting that without his staffers he was unable to make sense of what he was briefed on, and presumably whether it was legal in light of Congress' 1978 FISA statute or not. Of course, once the programs were revealed, the administration defended itself against a central criticism – that it had never so much as asked for modification of the FISA statute – by noting that key democrats in Congress were aware of the Program and raised no objection; Rockefeller's rather practical objection was easily overlooked by the public, and the classified briefing seemed in retrospect to be a clever way to preemptively tar natural opponents of the Program by association.

Finally, as noted previously, the fact that the leader of the Democratic party switched positions on the FAA statute in the summer of 2008 has meant that there is no partisan incentive to make surveillance an issue – instead, libertarian factions in both parties are pushing against their own member (Ron Wyden vs. Diane Feinstein, Rand Paul vs. Mike Rogers), in sharp

contrast to the partisan and libertarian furor over the NSA Program in 2006. Nonetheless, the closeness of recent votes in the House – likely a consequence of the polling patterns described above – indicates that Congress is not a lost cause notwithstanding all of these negatives.

***Minimization***

The Supreme Court's extension of Fourth Amendment protection to the content of phone calls is a relatively modern thing. Prior to 1967, precedent held that if the government didn't trespass onto your property in installing the bug there was no Fourth Amendment violation. The 1967 *Katz* decision changed this, holding that the content of a call was protected because individuals had "a reasonable expectation of privacy" in it (to use the formulation of Justice Harlan's famous concurrence).[52]

Congress responded to *Katz* by creating a statute to create ground rules whereby courts could issue warrants for wiretaps, but one basic problem was that, being a somewhat novel creature, the shape of what a Fourth-Amendment complaint warrant should look like was unclear. Whereas a traditional search warrant named the particular place to be searched and the specific items to be seized, a wiretap usually named a phone line to be bugged. And bugging a line is inherently a lot more open-ended and intrusive than searching a place for evidence related to a crime. Multiple people besides the target may use a line, the target may speak about private things unrelated to the crime under investigation, and in fact may even speak about privileged matters – conversations with his attorney being a prime example. And of course the tap is in place 24/7, and usually results in recording.

[52] [CITE Katz full and Harlan pin]

In a case called *Berger v New York*,[53] decided a few months before *Katz*, the Court specifically mentioned most of these problems and suggested that any warrant for wiretapping would need to meet higher standards, to be a super-warrant of sorts: wiretaps, being inherently intrusive, might only be justifiable at all in investigations of *serious* crimes. And they would require a variety of safeguards to ensure they were as narrow in concept as the physical search warrants the Founders envisioned: they would need to include time limits, the application should establish why no other method of evidence gathering would work, and, most importantly here, the application would need to provide for "minimization" – meaning, there would need to be procedures proposed for implementing the warrant that would protect against intercepting and recording things outside the scope of the warrant – irrelevant conversations – which would obviously include *privileged* conversations, like those of the target with his attorney.[54]

Minimization was a key to CCR's claims to standing for its legal staff plaintiffs in our 2006 litigation. The government argued that FISA surveillance would have been secret but just as harmful to us as surveillance under the NSA Program; our response was that even if the government could have convinced a judge to give it a warrant against the people we were communicating with abroad, there would have to be minimization procedures implemented that would protect our work-product or attorney-client privileged communications.[55] Despite the over 300 pages of briefing in the case, the government never responded to this argument.

Now we may know why: a DOJ memo published by the *Guardian*[56] indicates that the government's legal position seems to be that for foreign intelligence wiretaps, it only needs to

---

53 [CITE Berger – full]

54 [CITE Berger pin, and then other minimization-as-a-constitutional requirement cases]

55 Note that attorneys are protected by various legal communications privileges, but journalists are not. We had only attorney plaintiffs in our suits; the ACLU's similar suit included journalists. Consequently, the briefs (and thus the judicial rulings) in their case emphasized the minimization point somewhat less than our briefs did.

56 [CITE to story (not to memo)]

minimize out attorney-client conversations when the client is actually under indictment. So talking to family or fact or experts witnesses or co-counsel in, say, a Guantanamo habeas case, or in a pre-indictment counseling for someone located abroad like Julian Assange – these attorney communications, despite being clearly within the work-product or attorney-client privileges respectively, would not be subject to minimization. Rereading the various bits of evidence indicating that the NSA Program involved surveillance of attorneys in light of this narrow interpretation of legal privilege minimization simply amplifies our initial concerns. In sum, the likelihood is that the executive branch's implementation of minimization procedures provides far less protection for the most sensitive sorts of communications – attorneys with clients and other litigation participants – than we had previously believed was the case. And that in turn will continue to make it harder for litigators like us, working on national security cases of international scope, to sue over other illegal behavior of the executive branch.

Finally, it is worth noting that since the advent of Title III, the actual minimization procedures used by the FBI and other agencies have always been classified. This provides yet another avenue for the intelligence agencies to hide behind slippery, shape-shifting legal rationales: the idea that hidden minimization provisions exist and limit the application of a leaked surveillance order allows for a ready public-relations escape valve for the government anytime part of a legal rationale for surveillance comes to light, for the government can always claim that some hidden minimization procedures are at work narrowing how often a human agent views records. Indeed, David Kris speculated that the January 2007 orders that allowed the Bush administration to continue the initial NSA Program under FISC authorization were made possible only by strict minimization criteria implemented by the court (but, like the orders

themselves, entirely unseen by the public).[57] The paired Section 215 orders are an example of how a second order may contain provisions minimizing the impact of the first, broad collection order allowing compilation of the phone records database; the odd fact that the one first published by the *Guardian* contained no indication that the second order existed or limited its application will surely generate a certain amount of uncertainty about whether some as-yet-unseen minimization procedures mitigate in practice the impact of future leaked surveillance orders.

***Implications of long-term storage*** **[move this down nearer "Congress"?]**

One obvious concern for civil liberties in an era where mass surveillance data can be stored for long periods of time is that no one knows who will be president in four years. Nor do we know what political or religious associations may become suspect in the future – the Communist ties or Muslim community associations of some future generation. (Again, it is as realistic to think NSA could store all the data it gathers for very long periods as it is to think they could gather it in the first place.)

Another contribution to this symposium will address the history of warrantless broad-brush surveillance. [*John Mueller's piece] I will simply note a few points here: both republican and democratic presidents collected massive amounts of data on their political opponents in the civil rights and anti-Vietnam War movements. If it scares us to think that the FBI had dossiers on civil rights leaders and antiwar protesters in the 50s and 60s, today a far less transparent agency has dossiers on literally everyone. (ironically, James Comey's FBI directorship is term-limited to ten years because Congress was concerned to never allow the emergence of another J. Edgar

[57] [Chesney June 6 2013 lawfare posting]

Hoover, with dossiers on elected officials. Yet the NSA is using Congressional statutes to collect such information, potentially, on everyone.) Indeed, the new suit EFF has filed in federal court in California is centered on this idea: that mass-collection programs are a threat to associational freedom in the same way that Alabama's attempts to obtain the NAACP's membership lists were held to be in *NAACP v Alabama*.

***The intelligence/law-enforcement wall***

Proponents of untrammeled intelligence gathering by outward-directed foreign intelligence agencies like NSA have often claimed that one major protection our system offers targets is the "wall" built between intelligence gathering surveillance operations and surveillance carried out in support of criminal investigations. Putting to one side the complex question of what the nature of this separation is in the post-9/11 era, this claim boils down to the idea that that information gathered by these broadest NSA programs may never be used in court against the targets.

I would offer two responses: First, lawyers have an absolute obligation to protect client confidentiality, not just protect against the use of their communications in court against a client. As the various expert affidavits in our case and the ACLU chilling-effect cases indicated, we are obliged to protect confidentiality regardless of whether the confidence is ever used against the client in any forum. [Gillers words this so well – go back and check the original]

Second, the fact that intelligence is liable to be shared internationally raises separate concerns. To use an example from out 2006 case briefs: imagine we lawyers speak to family members of a Guantanamo detainee in Egypt. His family states that he is categorically opposed

to violence, and was merely a political opponent of the Mubarak regime. The U.S. intercepts and relays that information to Mubarak's government. The consequences would be dire, despite the fact that nothing discussed involves anything we would characterize as criminal behavior (at least in a *malum en se* sense). Clients and witnesses sensitive about either concern may simply not wish to participate in litigation, and cease communicating with us.

***Foreign government resistance as a check on U.S. spying***

Many of the most spectacular Snowden stories have involved accounts of NSA surveillance cracking into the email accounts of UN officials or foreign leaders like Felipe Calderón, or tapping into Angela Merkel's beloved and ever-present mobile handset.[58] To the extent people believe a lack of European cooperation with American surveillance will result, I suspect that is unlikely to happen for several reasons: first, many of these countries' executives may be happy to have the NSA share with them intelligence that they are restricted from gathering under their own laws. The likely outlet for the frustration over the Merkel scandal will likely be negotiation of some sort of bilateral no-spying-on-each-others-leaders arrangement[59] rather than a general effort to make it harder for NSA to spy within their countries generally. In addition, much of the infrastructure of global wired communications has been set up over the years such that major network pipelines transit the U.S., the geographical straightest-line-route rarely being a consideration when data flies at the speed of light. So, for instance, most

[58] [CITE three stories should do it here]

[59] [CITE But see, on the likelihood of such an arrangement with Germany or other non-historical intelligence allies, http://www.csmonitor.com/World/Security-Watch/2013/1028/US-spying-scandal-Why-Germany-and-France-won-t-get-Britain-s-deal-video and http://www.lawfareblog.com/2013/10/the-german-intelligence-agencies-are-coming-to-town/

communications from the Middle East to Asia move thru U.S. based switches.[60] Even if there were political will across the globe to resist NSA surveillance, the hardwiring of the system would take time to rework. And for mobile communications, which travel wirelessly over radio frequencies, resistance is nearly futile; U.S. spy stations in England can pick up signals from cell phones all throughout the continent.[61]

***Ineffectiveness: A natural check?***

President Obama has proclaimed himself eager to debate the "balance of liberty and security" implicated by these surveillance programs. Of course, the very terms of that debate presume that there is always a tradeoff involved – that safeguards, typically coming in the form of judicial review, always will operate to diminish security. The public tends to think of courts as primarily serving to throw a monkey wrench into the gears of law enforcement's efforts to gather evidence, as yet another mechanism whereby one branch slows down the work of another.

Even putting aside all practical experience, it is odd to believe this in theory. When we require the executive to show up in court and prove with some small quantum of evidence that there is reason to suspect the target of being worthy of surveillance, judicial oversight isn't a burden to the system – instead, it results in more efficient law enforcement because it focuses law enforcement's efforts on threats that are real. For 200-plus years having judges review the evidence for "probable cause" before issuing search warrants is a system that has worked to ensure not only that the innocent don't get searched, but also that law enforcement doesn't waste its time with irrational profiling.

---

60 [CITE Risen, State of War ch.2?]

61 [CITE Keefe book – NB my copy may be in Providence right now]

Our historical experience with warrantless surveillance confirms this. Inefficiency has been a hallmark of warrantless surveillance since the Church Committee reports, which showed that Presidents Nixon and Johnson targeted their political opponents (in the civil rights and Vietnam War protest movements). "Duplication, waste, and inertia" were the conclusions of one part of the Committee's reports on what happened when the agencies were allowed to gather information without any effective outside oversight. Whenever we removed courts as agents of accountability and oversight, we got lazy law enforcement.

Mass surveillance of the scope described in the Snowden documents should present other problems in theory as well. Gen. Alexander's claim that the NSA seeks to "collect everything" implicitly assumes that size of the data pool gathered equals success. But intelligence experts themselves have long warned of the danger that the more data you collect, the more chaff there is hiding the kernels of wheat, the more haystack hiding the needle. (Alexander's response to this before Congress was: "You need the haystack to find the needle," which perhaps only proves that the actual meaning of farm metaphors is lost on high-tech executives.)

The *New York Times* and *Washington Post* reported very early on in 2006 that the *targeted* NSA Program produced lots of bad leads that were passed on to the FBI for further investigation, resulting in both dead ends – "more calls to Pizza Hut," in the words of an FBI agent quoted in the Times' story – and, of course, the lost opportunity costs of the wasted effort in pursuing those leads to being with.[62] (Curiously, the only reason this evidence of the poor practical efficacy of the NSA Program came out in 2006 was likely that natural interagency rivalries gave the FBI an incentive to leak information to reporters – a dynamic that seems to have played out between the FBI and CIA throughout various torture-related FOIA releases.)

[62] Lowell Bergman, Eric Lichtblau, Scott Shane and Don Van Natta Jr., *Spy Agency Data After Sept. 11 Led F.B.I. to Dead Ends*, N.Y. Times (Jan. 17, 2006); [CITE WaPo story near same time cited in longform SOTU TP document]

The *Washington Post* has similarly unearthed and published a slide revealing some of the NSA's current over-collection problems: because spammers got into an email account the agency was surveilling, the web of connections from sent emails out of that compromised account became so huge it was flooding their entire collection system, eventually forcing NSA to cut off that target from surveillance. (Perhaps the lesson for civil libertarians here is to periodically click on those Nigerian emails to protect your gmail account from surveillance.)[63]

In 2006 only a small handful of dubious success stories were advertised by the NSA as proof that the Program worked (with claims that dossiers on amateurish jihadists Mohammed Junaid Babar and Iyman Faris were augmented in part thru the program). Similarly, there are very few examples that the NSA has even tried to hold out as successes for what are surely multi-billion dollar programs. The NSA claims that the identification of 2009 subway bomb plotter Najibullah Zazi traces back to an intercepted email he sent to the Yahoo account of a known al Qaeda figure in Pakistan – in other words, an account the pre-2007 version of FISA would have readily facilitated surveillance of, and one already being watched by British intelligence.[64] British intelligence also first found David Coleman Headley, another find claimed for the NSA. NSA claimed the call records database helped lead them to Basaaly Moalin, convicted of material support for sending funds to al Shabab; like Zazi, the agency used a Shabab member's number as the starting point, and could have done a conventional investigation via particularized court order from that first clue. Finally, an FBI official told CBS that several Americans, one of whom plead guilty three years ago to material support for al Qaeda, had plotted to bomb the NYSE, an attack detected in advance by NSA – but there is no evidence

---

63 http://apps.washingtonpost.com/g/page/world/the-nsas-overcollection-problem/517/

64 Matt Apuzzo and Adam Goldman, NYC Bomb Plot Details Settle Little in NSA Debate, AP (Jun. 13, 2013) http://bigstory.ap.org/article/nyc-bomb-plot-details-settle-little-nsa-debate

beyond that statement that this plot was in any way real.[65] This very thin case for efficacy is probably why Gen. Alexander by September had begun to frequently advertise national "cyber security" as an additional justification for the mass collection programs.

Alexander has spoken of the "peace of mind metric"[66] with respect to mass surveillance: at least we have everything, even if it's not easy to use! But even saying that seems in a way an acknowledgment that the current system doesn't work well. Surely the agency understands this at some level. Why keep doing it, then? On possibility – which we proposed even back in 2006 – is that the goal of gathering these haystacks is to enable the retrospective testing of technologies developed in the future to sort them. On this theory, these databases are gathered mainly so as to allow the NSA to test various algorithms designed to spot possible threats based on nothing more than patterns of communication – that one call from Afghanistan in the middle of night followed by ten calls out described *supra*. Such algorithms can only really be tested to see if they "work" by running them against a past database and seeing if they spot threats that proved to exist when an attack happened or was preempted by more traditional intelligence gathering and law enforcement techniques.

Such an aspiration would fit into one long-term dream of the intelligence agencies: to replace the human element of intelligence operations, which has historically proven to be inherently flaky, expensive, and prone to working for the enemy, with machine intelligence – ever-refined until it proves foolproof, the Manchurian candidate of the intelligence field. The mindset would also be consistent with the entrepreneurial atmosphere that seems to prevail within the NSA, based on the Snowden documents: multiple programs, constantly turning over,

---

[65] Justin Elliott and Theodoric Meyer, *Claim on "Attacks Thwarted" by NSA Spreads Despite Lack of Evidence*, ProPublica (Oct. 23, 2013), *available at* www.propublica.org/article/claim-on-attacks-thwarted-by-nsa-spreads-despite-lack-of-evidence.

[66] [CITE]

competing over similar functionality, brassily advertising themselves. "[T]he allure of big data"[67] is everywhere today, but machine intelligence might also have seemed like a ready solution to one of the many intelligence crises posed by 9/11: that we had far too few human intelligence resources already in place in the Arab world the day after the attacks.

Such a system, when perfected, would in theory aspire to intercept as much data of every variety in bulk first and find suspects later, rather than starting with evidence generating suspicion and investigating those specific targets – the traditional preemptive law enforcement model of seeking out the tip of the conspiratorial iceberg and then throwing more assets at traditional techniques (targeted intercepts, tailing, infiltration) to uncover the hidden mass below the waterline. The problem with this aspiration *in theory* is that it assumes an algorithm can be found which generates almost no false positives. An algorithm that produces an infinitesimal rate of false positives, when applied to a massive database, will overwhelm any system with "more calls to Pizza Hut." Indeed any algorithm, to be useful in practice, must produce an almost negligible false positive rate because the ratio of false positives against hits must be small, and the number of actual terrorist conspirators in any society is itself infinitesimal. [Pull the second-week WSJ story on prediction rates from Westlaw and the Economist story the same week]

I've already noted above that many commentators believe that because the Fourth Amendment warrant clause and its particularity requirements are so inherently incompatible with mass surveillance, such data mining programs will eventually only be reviewed for "reasonableness" under the first generally-applicable clause of the Amendment, which states that "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated." But there is also an antecedent question, which is whether a *computer* searching your data without ever flagging it for review by

[67] [Alex Abdo's ACLU blog]

a human operator even constitutes a "search." [CITE Kerr et al. papers; maybe add a sentence or two of elaboration.] On this theory, if NSA is only exposing records to scrutiny by human agents after it has been flagged by a computer algorithm, then the millions of records the algorithm scans and rejects have not been searched, and even the reasonableness requirement may not apply to them. The ACLU call-records plaintiffs base their standing on the fact that *all* records of subscribers to their telecom provider have been turned over to the NSA, including of course theirs, but if all those records have only been scanned by a computer for ties to one of the 300 target numbers queried, then under this theory for exempting machine searches, it is unclear that their records have been "searched" for Fourth Amendment purposes.

Finally, any such system, no matter how sophisticated, would be easy to avoid if terrorist conspirators simply took a low-tech approach. Recall that by the afternoon of 9/11 there were already pundits on the networks announcing that soon the public would hear about how the plotters pulled it off with encryption. Instead, they used the most primitive of techniques: staying off-grid, communicating in code when they did use email (from public computer terminals), etc.[68] As Newsweek summarized it, "[t]he NSA's top brass assumes that if a threat does not show up in its databases, it doesn't exist. As one woman who lives online, Marcy Wheeler, said, the next terrorist attack will come from a group that stays offline 'and we're going to be hit bad by it because we have this hubris about the degree to which all people live online.'"[69]

***Self-help***

[68] In fairness, Zazi did as well, but got caught, his email correspondent already being a marked man and his choice of code words too commonplace. *See* Goldman and Apuzzo, *supra* note 64.

[69] http://mag.newsweek.com/2013/10/04/the-woman-who-knows-the-nsa-s-secrets.html

"Strong encryption works":[70] no less an authority than the famously-paranoid Edward Snowden has said as much. While almost all commercial software packages must be assumed to be vulnerable in the same way the 256-bit AES encrypted Skype is, simple, negligible-cost combinations of open-source programs like Jabber (chat) and Jitsi (video) paired with PGP encryption can replace most commercial means of electronic communication. Whereas the previous suspicion that encrypting communications simply flagged them for the NSA (which, according to some reports, stores all the encrypted communications it encounters for such date in the future as computing power makes it more convenient to decode them), one consequence of Snowden's revelations will likely be that larger numbers of commercial and noncommercial users routinely encrypt electronic communications. At the very least, encryption buys time against the government.

***Statutory limits, Congressional self-interest, and some concluding thoughts***

While I've voiced skepticism about the potential for FISC reform to significantly affect our current situation, Congress could certainly impose meaningful limits on the NSA by statute. It could revoke the broad authority granted by the FAA, impose a warrant progress for government access to third-party records, bar long-term storage of data – almost every problem noted above could be addressed by statute. FISA itself occupied an effectively unregulated space when it was passed in 1978. Nor is it fantasy to think such things might happen in the near term. The first post-Snowden bill, pushed by Representatives Conyers and [check] Nadler in the House, came close to passing, and some Tea Party libertarians seem to be promising (if unfamiliar) bedfellows here.

[70] [CITE]

That brings me to one final thought on all of this: To what extent are judges, members of Congress and other elected officials exempted from NSA surveillance? If they are not, the chilling effect that afflicts attorneys and journalists applies here as well and has similarly-enormous potential to corrupt the political process. Imagine Anthony Weiner hadn't accidentally mass-tweeted that fateful photograph, and had remained in the House, but knew that the NSA knew about his habits – and was casting the deciding vote on a bill limiting the powers of the NSA?

Such a scenario is not entirely the stuff of fiction: FBI director J. Edgar Hoover had accumulated dossiers on all sorts of elected officials, which is why James Comey's term in that same office has been limited to ten years by statute – to avoid allowing any future FBI director to accumulate that much dirt on (and accompanying passive leverage over) Congressmen. Even Supreme Court justices had been surveilled in the past, as the Church Committee discovered. Perhaps one consequence of the accumulation of private conversations from foreign leaders' cell phones and email accounts will be not to undermine their negotiating positions at the G20 or the UN directly, but to allow the accumulation of leverage by discovering embarrassing secrets in their closets. Either way, the potential for surveillance corrupting the political process extends to multinational negotiations between democracies as well.

Interestingly, Snowden did a two-hour-long live chat with *Guardian* readers from Hong Kong, which he ended by noting (in response to Glenn Greenwald's final "anything else you'd like to add" question) that: "The US Person/foreigner distinction is not a reasonable substitute for individualized suspicion, and is only applied to improve [political] support for the program. This is the precise reason that NSA provides Congress with a special immunity to its surveillance."[71]

[71] *Edward Snowden: NSA whistleblower answers reader questions*, The Guardian (Jun. 17, 2013), http://www.theguardian.com/world/2013/jun/17/edward-snowden-nsa-files-whistleblower

Snowden's first sentence neatly summarizes the polling data I described earlier. The second illustrates the potential scope for corruption of the democratic process posed by sweeping content and metadata surveillance, whether or not Congress is exempted from some or all of it. Mass surveillance of this all-seeing scale, with the government able to assemble together everything about us that exists outside of our heads – all of our consumer activities, all of our communication patterns and other social connection –is arguably fundamentally incompatible with democratic self-governance also. One reason the Framers paid so much attention to protecting property rights from the state is that they thought private property ensured autonomy from the state; give the government sufficient power to control wealth and the means to produce it, and the people wouldn't be independent enough to control the government. Essentially, to have a democracy, you need the citizenry to be somewhat autonomous from government, independent of all-encompassing government control. Mass surveillance threatens that independence enough to corrupt democracy itself. When the government "can literally see your thoughts form as you type,"[72] your degree of control over government is at the very least limited by the same sort of self-censorship that afflicts the lawyers and journalists who first sued over these NSA Program in 2006.

I think a lot of today's voters actually understand that at some deep level. So that makes it strange that the most commonplace excuse for not caring about mass surveillance is that old saw: "ordinary Americans have nothing to fear." And I suppose at some level, that's just it. The existence of a program like this is a tremendous disincentive to participate in anything this government doesn't like, or, for the more far-sighted, that some future government may not like.

---

[72] Barton Gellman & Laura Poitras, *U.S., British intelligence mining data from nine U.S. Internet companies in broad secret program*, Wash. Post (Jun. 6, 2013), available at 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.

Put another way, it's a huge incentive to become more ordinary in one's political, socioeconomic, and even religious beliefs. Why go to an animal rights conference, join a Google group of like-minded people opposed to the WTO, protest the next war in the streets, knowing that tomorrow the government may regard these associations as suspect and track them back to you? The most succinct statement of the homogenizing potential of such an all-seeing government was made by Umair Haque, who asked: "Can there be a more chilling message to conform than 'America is not interested in spying on *ordinary* people'"?[73]

[73] [CITE to his Twitter feed (emphasis added).] [Perhaps an amusing point to note that the Library of Congress is apparently archiving all of Twitter (how's this deal with blocked viewers etc.?).]

Publication forthcoming in:
I/S: A Journal of Law and Policy for the Information Society (www.is-journal.org)
10 ISJLP ___ (2014)
Draft version, subject to revisions

# THE MASSIVE METADATA MACHINE: LIBERTY, POWER, AND ~~SECRET~~ MASS SURVEILLANCE IN THE U.S. AND EUROPE

Bryce Clayton Newell, J.D.
The Information School, University of Washington (Seattle)

## Abstract

*This paper explores the relationship between liberty and security implicated by secret government mass surveillance programs. It includes both doctrinal and theoretical analysis. Methodologically, the paper examines judicial reasoning in cases where parties have challenged secret government surveillance programs on Constitutional or human rights grounds in both United States' Courts and at the European Court of Human Rights (ECtHR). Theoretically, this paper will draw on theories in the fields of law, surveillance studies, and political theory to question how greater recognition of citizen rights to conduct reciprocal surveillance of government activity (for example, through expanded rights to freedom of information) might properly balance power relations between governments and their people. Specifically, the paper will question how liberal and neo-republican conceptions of liberty, defined as the absence of actual interference and the possibility of arbitrary domination, respectively, and the jurisprudence of the ECtHR can inform the way we think about the proper relationship between security and liberty in the post-9/11, post-Snowden United States of America.*

# Table of Contents



## I. INTRODUCTION

Because information can provide and facilitate power, the collection and use of large amounts of information (including communications metadata) can significantly impact the relationships between governments and their citizens.[1] Access to information is often a prerequisite to exercising power or seeking redress for potential rights violations stemming from secret activities of others.[2] As such, an imbalance in information access between a people and their government can tip the scales of power and limit the ability of the people to exercise democratic oversight and control those they have put in power to represent them.[3] Freedom of information (FOI) laws often provide a great deal of access to government records and serve as a powerful and effective means for empowering oversight by journalists and ordinary citizens. In a very real sense, these laws provide a legal mechanism for citizen-initiated surveillance from underneath

[1] *See* Craig Forcese and Aaron Freeman, THE LAWS OF GOVERNMENT: THE LEGAL FOUNDATIONS OF CANADIAN DEMOCRACY 481-84 (Irwin Law, 2005).

[2] *Id.*

[3] *Id.*

(sometimes termed "sousveillance"[4] or the "participatory panopticon"[5]). This form of reciprocal surveillance (which may take numerous forms) grants citizens greater power to check government abuse and force even greater transparency.[6] However, as the recent and on-going battle for greater transparency at the United States' Foreign Intelligence Surveillance Court (FISC) demonstrates, most government records related to mass surveillance for foreign intelligence purposes are strictly guarded, classified, and kept from the people almost *in toto*, even when all such records might not actually reveal information that could harm the county's national security interests.

Edward Snowden's decision to leak classified intelligence documents to the press in 2013 certainly reinvigorated national and international critique of large-scale surveillance programs, but the controversies are not really all that new. Cross-border intelligence sharing between the global "Five-Eyes" countries (the USA, UK, Canada, Australia and New Zealand) has been acknowledged for years, despite the NSA only recently declassifying certain historical documents about the UKUSA agreement and its early predecessors in the aftermath of the Second World War. These collaborative efforts encompass a truly global infrastructure, and they are undoubtedly highly effective at neutralizing a variety of national security threats. They also pose some difficult questions for democratic governance and individual liberty.

For example, cross-border information sharing without strict and clearly worded regulations may potentially allow governments to evade domestic restrictions on directly collecting intelligence information about their own citizens. In addition, the recent revelations reinforce the fact that governments are maintaining arguably outdated legal standards about the differences between metadata – or information about information – and the substantive contents of communications. These legal allowances for substantial metadata surveillance pose serious risks to individual privacy and, given the modern reality that information equals (or at least facilitates) power, potentially allow governments to impermissibly interfere with individual liberty and, ultimately, to arbitrarily dominate the citizenry they are supposed to represent.

---

[4] *See* Steve Mann, Jason Nolan, and Barry Wellman, *Sousveillance: Inventing and Using Wearable Computing Devices for Data Collection in Surveillance Environments*, 1 Surveillance & Society 331 (2003), *available at* http://library.queensu.ca/ojs/index.php/surveillance-and-society/article/view/3344/3306; Jean-Gabriel Ganascia, *The Generalized Sousveillance Society*, 49 Social Science Information 489 (2011).

[5] Jamais Cascio, *The Rise of the Participatory Panopticon*, World Changing, May, 4, 2005, at http://www.worldchanging.com/archives/002651.html; Mark A. M. Kramer, Erika Reponen and Marianna Obrist, *MobiMundi: exploring the impact of user-generated mobile content – the participatory panopticon*, Proceedings of the 10th International Conference on Human Computer Interaction with Mobile Devices and Services (MobileHCI '08), pp. 575-577 (2008).

[6] David Brin, THE TRANSPARENT SOCIETY: WILL TECHNOLOGY FORCE US TO CHOOSE BETWEEN PRIVACY AND FREEDOM? (Perseus Books, 1998; Kevin D. Haggarty and Richard V. Ericson, *The New Politics of Surveillance and Visibility* 10 (K.D. Haggarty. & R.V. Ericson eds., THE NEW POLITICS OF SURVEILLANCE AND VISIBILITY, University of Toronto Press, 2006).

This paper explores the relationship between liberty and security implicated by secret government surveillance programs, with an emphasis on the U.S. experience. It includes both doctrinal analysis of case law in the United States and at the European Court of Human Rights (ECtHR) as well as theoretical analysis informed by political theory and literature within the burgeoning field of surveillance studies. Methodologically, the paper examines judicial reasoning in cases where parties have challenged secret government surveillance programs on Constitutional or human rights grounds. In doing so, this paper will question how liberal and neo-republican conceptions of liberty, defined as the absence of actual interference and the possibility of arbitrary domination, respectively, can inform the way we think about the proper relationship between security and liberty in the post-9/11, post-Snowden world. This paper will also explore how needed legal protections for non-content information (metadata) can effectively aid in reducing the potential of government domination.

This paper concludes that governments must allow their citizens enough access to information necessary for individual self-government and that greater protections for some types of metadata and aggregate communications data may need to be implemented to effectively reduce the risk of actual interference and arbitrary domination. To be fully non-arbitrary and non-dominating, government must also respect and provide effective institutional and legal mechanisms for their citizenry to effectuate self-government and command noninterference. Establishing liberal access rights to information about government conduct and mechanisms that ensure that citizens can effectively command noninterference are justified on the grounds that they reduce the possibility of arbitrary, and actual, interference with the right of the people govern themselves. Such measures would also limit the institutionalization of systemic domination within political and social institutions. In an age when technology has "changed the game"[7] by removing barriers to the government's ability to access, aggregate, and utilize the personal information of the people, the law should similarly adapt and provide citizens with rights to counter the otherwise inevitable power imbalance, through greater privacy protections and/or enhanced access to government information.

## II. MASS SURVEILLANCE AND NATIONAL SECURITY

Mass surveillance is not entirely new, although advances in technology continue to supplement the abilities of governments to gather greater amounts of information much more efficiently. Additionally, cross-border intelligence operations and information-sharing between domestic and foreign intelligence agencies is a long documented reality. Recent revelations that the National Security Administration (NSA) has been sharing raw, un-redacted, intelligence information (including information about American citizens) with Israel with few strings attached[8] may have

[7] Adam D. Moore, PRIVACY RIGHTS: MORAL AND LEGAL FOUNDATIONS 4 (Penn State Press, 2010).

[8] Glenn Greenwald, Laura Poitras and Ewen MacAskill, *NSA shares raw intelligence including Americans' data with Israel*, The Guardian, Sept. 11, 2013, at http://www.theguardian.com/world/2013/sep/11/nsa-americans-personal-data-israel-documents.

surprised some, but is consistent with the historical trajectory of cross-border intelligence sharing by the NSA and its predecessors.

International signals intelligence (SIGINT) sharing owes its roots, at least in part, to a British-USA intelligence sharing arrangement, later formalized as the "BRUSA" Circuit and then the UKUSA Agreement, which began to take shape as early as 1940, when the British government requested the exchange of secret intelligence information and technical capabilities with the United States.[9] This information-sharing association is often now referred to as Echelon or "Five Eyes." In the 1940s, the two countries negotiated a number of agreements related to intelligence cooperation and information sharing, establishing a formal agreement on communications intelligence (COMINT) sharing in March of 1946.[10] In 1955 and 1956, the relationship was further formalized in an updated UKUSA agreement, which also included reference to the inclusion of Canada, Australia, and New Zealand as "UKUSA-collaborating Commonwealth countries."[11] Subsequent agreements and documents have not been declassified, however, but the continuing existence of the "Five Eyes" partnership has been confirmed.

The early UKUSA agreement was limited to COMINT matters (a subset of the larger category of SIGINT, which also includes electromagnetic intelligence – or ELINT) and collateral material "for technical purposes."[12] Under the agreement, the national agencies pledged to exchange the following COMINT products: 1) collection of traffic, 2) acquisition of communications documents and equipment, 3) traffic analysis, 4) cryptanalysis, 5) decryption and translation, and 6) acquisition of information regarding communications organizations, procedures, practices and equipment.

The United States and many other countries have also subsequently entered into treaties with a number of foreign states to share information and assist foreign law enforcement agencies to investigate and prosecute crime and terrorism. Generally, these agreements are called mutual legal assistance treaties (MLATs). As an example, Canada and the United States signed a Mutual Legal Assistance Treaty (the "CAN-US MLAT") in 1985 which focused on cooperation

[9] The United States National Security Agency has released declassified documents related to the early UKUSA agreement on its website at http://www.nsa.gov/public_info/declass/ukusa.shtml; the early papers, including the initial request from the British Embassy proposing the information sharing arrangement, can be found in Early Papers Concerning US-UK Agreement – 1940–1944, available at http://www.nsa.gov/public_info/_files/ukusa/early_papers_1940-1944.pdf.

[10] British-U.S. Communications Intelligence Agreement and Outline – 5 March 1946, available at http://www.nsa.gov/public_info/_files/ukusa/agreement_outline_5mar46.pdf.

[11] New UKUSA Agreement – 10 May 1955, available at http://www.nsa.gov/public_info/_files/ukusa/new_ukusa_agree_10may55.pdf.

[12] *Id.* at § 2 of the UKUSA Agreement (page 5 of the PDF).

in criminal matters.[13] The CAN-US MLAT, which is similar in many regards to treaties with other countries, provides that the two countries shall provide "mutual legal assistance in all matters relating to the investigation, prosecution and suppression of offences,"[14] including "exchanging information… locating or identifying persons… providing documents and records… [and] executing requests for searches and seizures."[15]

In the years between 9/11 and Edward Snowden's leaking documents to the press in 2013, national communications and foreign intelligence programs changed from a "need to know"[16] mentality to a "new culture of 'need to share.'"[17] As then Director of National Intelligence Dennis Blair noted in his Preface to the 2009 National Counterintelligence Strategy, information sharing has led to greater vulnerabilities, which requires greater collaboration and coordination between intelligence agencies.[18] Based on Snowden's recent revelations and earlier reports, we know that government agencies, and particularly the NSA, have been collecting and analyzing vast quantities of telecommunications metadata as well as other online information from social media and online communications providers for quite some time.

## III. THE (META)DATA PROBLEM

Metadata, commonly defined as "information about information," includes (in the context of electronic communications) information about the time, duration, and location of a communication as well as the phone numbers or email addresses of the sending and receiving parties. It also may include information about the device used (make/model and specific device identification number). Metadata is generated whenever a person uses an electronic device (such as a computer, tablet, mobile phone, landline telephone, or even a modern automobile) or an electronic service (such as an email service, social media website, word processing program, or search engine). Often, this results in the creation of considerable amounts of information (metadata). In most cases, service providers collect and retain this information in databases that often can be traced directly to an individual person.

---

[13] Treaty between the Government of Canada and the Government of the United States of America on Mutual Legal Assistance in Criminal Matters (hereinafter "CAN-US MLAT"), E101638 - CTS 1990 No.19, March 18, 1985, available at http://www.treaty-accord.gc.ca/text-texte.aspx?id=101638.

[14] *Id.* at art. II, § 1.

[15] *Id.* at art. II, §§ 2(b), (c), (f), and (h).

[16] THE 9/11 COMMISSION REPORT: FINAL REPORT OF THE NATIONAL COMMISSION ON TERRORIST ATTACKS UPON THE UNITED STATES, at p. 417 (official govt. ed. 2004).

[17] Peter P. Swire, *Privacy and Information Sharing in the War on Terrorism*, 51 Vill. L. Rev. 951, 951 (2006), *citing* 9/11 Commission Report, *supra* note 13, at 417.

[18] Dennis C. Blair, *Preface* to the National Counterintelligence Strategy of the United States of America, at p. iii (official govt. ed. 2009), available at http://www.ncix.gov/publications/strategy/docs/NatlCIStrategy2009.pdf.

But metadata is not just associated with electronic communications, it also serves to document various properties of other facts, documents, or processes. For example, automated license plate recognition systems create metadata about the locations of vehicles at certain points in time. Taking a digital photograph often creates metadata about the location the photograph was taken, the aperture, focal length, and shutter speed settings of the camera. Word processing programs such as Microsoft Word also save metadata such as the name of the author who created the document, the date of creation, the date on which the latest changes have been made, the name of the user who made the most recent changes, the total number of words and pages in a document, and the total length of time that a document has actually been edited.

### *a. METADATA AND SURVEILLANCE AFTER EDWARD SNOWDEN*

After Edward Snowden leaked classified NSA documents to the press in mid-2013, questions about the nature of government collection of communications metadata took a prominent place on the world stage. Snowden's first revelation was a classified court order from the secretive U.S. Foreign Intelligence Surveillance Court (FISC) that compelled Verizon, one of the largest U.S. telecommunications providers, to provide the U.S. government with all of its customers' telephone metadata on an ongoing basis – encompassing landline, wireless and smartphone communications. Other disclosures indicate that the three major U.S. telecommunications companies were subject to similar orders[19] and that NSA surveillance covered approximately 75% of all Internet traffic in the U.S., including email.[20]

In a Congressional hearing, top U.S. officials claimed that they were only collecting information about numbers of the parties to communications (the sender and receiver of phone calls) and the duration of the calls. NSA and Justice Department officials, and high-ranking Congressional representatives, also claimed that since they were not collecting the actual contents of communications (e.g. the words spoken), the surveillance did not invade anyone's reasonable expectations of privacy. The officials claimed explicitly that they were not collecting geolocation data (e.g. the geographic location of the device when the call was made or received),[21] but nothing in the FISC order limited the government from obtaining this kind of information as well. Importantly, the U.S. authorities are only legally restricted from collecting the actual contents of Americans' communications under the U.S. Constitution, as they are

[19] Siobhan Gorman , Evan Perez, and Janet Hook, *U.S. Collects Vast Data Trove*, Wall Street Journal, June 7, 2013, at http://online.wsj.com/article/SB10001424127887324299104578529112289298922.html. For some historical precedent, also see Leslie Cauley, *NSA has massive database of Americans' phone calls*, USA Today, May 11, 2006, at http://usatoday30.usatoday.com/news/washington/2006-05-10-nsa_x.htm.

[20] Barry Ritholtz, *New Details Show Broader NSA Surveillance Reach*, Wall Street Journal, Aug. 21, 2013, at http://online.wsj.com/article/SB10001424127887324108204579022874091732470.html (behind paywall).

[21] *See* Adam Serwer, *Is the NSA collecting cell phone location data?*, MSNBC.com, Sept. 27, 2013, at http://tv.msnbc.com/2013/09/27/is-the-nsa-collecting-cell-phone-location-data/; *see also* Paul Lewis and Dan Roberts, *US intelligence chiefs urge Congress to preserve surveillance programs*, The Guardian, Sept. 26, 2013, at http://www.theguardian.com/world/2013/sep/26/nsa-surveillance-senate-committee.

legally permitted to collect the contents (and metadata) of non-U.S. persons around the world without any prior judicial authorization.

### *b. Problems with Binary Fourth Amendment Theory*

Much of the metadata surveillance conducted by the NSA, including the harvesting of telephone records of U.S. citizens, is permitted, legally, based on Supreme Court decisions about the appropriate expectation of privacy that individuals may hold in "non-content" (metadata) information.[22] These cases held that citizens cannot claim privacy interests, *vis-à-vis* the government, in records turned over to a third-party (bank records)[23] or in the numbers dialed from a telephone.[24] As a consequence, legal definitions of privacy (at least in the Fourth Amendment search context) have often been crafted to force conclusions about potential privacy violations based on binary distinctions: either a form of investigation or information gathering by government agents constitutes a search or it does not.[25] The binary nature of this analysis itself is not inherently problematic – in fact it may be highly desirable to draw clear lines governing law enforcement action. However, certain strict application of binary tests developed in past cases, without reconsideration of the rapid developments in information technologies and the scope of possible government intrusion into private life through massive metadata acquisition programs, may improperly restrict Fourth Amendment protections of personal privacy.

A recent FISC decision[26] upholding the constitutionality of the FBI/NSA telephone metadata surveillance program authored by Judge Claire Egan and released on September 17, 2013, failed to take account of potentially important dicta in Supreme Court's decision in *United States v. Jones*.[27] In that case, the Justices held that the warrantless application of a GPS tracking device to a suspect's automobile violated the suspect's Fourth Amendment rights. In two concurring

---

[22] *See* Smith v. Maryland, 442 U.S. 735 (1979); United States v. Miller, 425 U.S. 435 (1976). For a recent FISC decision reaffirming this point, see Amended Memorandum Opinion, In Re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things from [redacted], Docket No. BR 13-109 (as amended and released on Sept. 17, 2013) (opinion of Judge Claire V. Egan) (hereinafter "Egan Opinion"), available at http://www.uscourts.gov/uscourts/courts/fisc/br13-09-primary-order.pdf; *see also* D'Andrea, 497 F. Supp. 2d 117, 120 (U.S.D.C. Mass., 2007); Guest v. Leis, 255 F.3d 325, 336 (6th Cir. 2001) (holding that a user loses any expectation of privacy in personal subscription information when it is conveyed to a system operator); United States v. Cox, 190 F. Supp. 2d 330, 332 (N.D.N.Y. 2002) ( "[C]riminal defendants have no Fourth Amendment privacy interest in subscriber information given to an internet service provider ." ); Bryce Clayton Newell, *Rethinking Reasonable Expectations of Privacy in Online Social Networks*, 17 Rich. J.L. & Tech., art. 12, p. 32 (2011), http://jolt.richmond.edu/v17i4/article12.pdf.

[23] United States v. Miller, 425 U.S. 435 (1976).

[24] Smith v. Maryland, 442 U.S. 735 (1979).

[25] *See* Orin Kerr, *The Mosaic Theory of the Fourth Amendment*, 111 Michigan L. Rev. 311 (2012).

[26] Egan Opinion, *supra* note 22.

[27] United States v. Jones, 132 S. Ct. 945 (2012).

opinions signed by five justices, Justices Sotomayor and Alito separately argued that aggregated geo-locational metadata ought to raise a reasonable expectation of privacy.[28]

Because of the concurring opinions in *Jones*, which signal the possibility that a majority of the Justices might be open to revisiting Fourth Amendment theory in light of modern technologically-aided police practices,[29] it may be an opportune time to argue for a normative approach to privacy in Fourth Amendment jurisprudence that is more sensitive to context (not bound by purely binary distinctions) and the increasingly revealing capacity of metadata surveillance, especially when such information is collected, stored, and mined in the aggregate.

## IV. SECRET SURVEILLANCE CASE LAW: THE U.S. AND EUROPE

Courts around the world have grappled with the legal issues implicated by secret government surveillance programs for a number of years. The two succeeding sections provide an overview of some of the important cases in the United States and at the European Court of Human Rights (ECtHR).

### *a. THE EUROPEAN COURT OF HUMAN RIGHTS*

The ECtHR has a long history of decisions questioning whether secret government surveillance is conducted consistent with the provisions of Article 8 of the European Convention on Human Rights (the "Convention").[30] In comparison to the United States, the Convention acts (along with individual State constitutions) as one European corollary to the U.S. Constitution as a basic limit on government authority to conduct domestic (and international) surveillance, albeit at a supranational level.

The first relevant ECtHR case is *Klass and Others v. Germany*[31] from 1978. In that case, Klass and four other applicants challenged provisions of a German surveillance statute on two primary grounds; first, that the act did not require the government to notify targets of surveillance after the surveillance had concluded and, second, that the act excluded remedies before regular domestic courts.[32] Ultimately, the ECtHR found no violation of the applicants' Article 8 rights, but the Court outlined the relevant test to determine when secret surveillance powers might

[28] See *id.* (concurrence of Justice Sotomayor and concurrence of Justice Alito).

[29] Kerr, *supra* note 25, at 320 ("A close reading of *Maynard/Jones* suggests that five Justices are ready to embrace the new mosaic approach to the Fourth Amendment: Justices Ginsburg, Breyer, Alito, Kagan, and Sotomayor.")

[30] The primary cases cited in ECtHR jurisprudence are *Klass and Others v. Germany*, [1978] ECHR 4 (hereinafter "Klass"); *Malone v. United Kingdom*, [1984] ECHR 10 (hereinafter "Malone"); *Weber and Saravia v. Germany*, [2006] ECHR 1173 (hereinafter "Weber"); *Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria*, [2007] ECHR 533 (hereinafter "Ekimdzhiev"); *Liberty and Others v. United Kingdom*, [2008] ECHR 568 (hereinafter "Liberty"); and *Iordachi and Others v. Moldova*, [2009] ECHR 256 (hereinafter "Iordachi").

[31] *Klass*, *supra* note 30.

[32] *Id.* at paras. 10, 26.

violate a person's basic human rights. This test has been largely adopted in recent cases, with some modifications (including more restrictive requirements when determining whether conduct is "in accordance with law").

Article 8 of the Convention states (in relevant part):

> "1. Everyone has the right to respect for his private and family life, his home and his correspondence.
>
> 2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society…."[33]

The applicants in *Klass* were lawyers who regularly represented individuals they suspected of being under surveillance. These attorneys concluded that their own communications might also have been intercepted, and initiated claims to challenge the surveillance as a violation of their Article 8 rights. The European Commission on Human Rights (the "Commission") declared the application admissible to the ECtHR, essentially holding that the applicants had standing. Despite the fact that only "victims" of alleged violations of the Convention could bring cases before the ECtHR, the Commission found that,

> "As it is the particularity of this case that persons subject to secret supervision by the authorities are not always subsequently informed of such measures taken against them, it is impossible for the applicants to show that any of their rights have been interfered with. In these circumstances the applicants must be considered to be entitled to lodge an application even if they cannot show that they are victims."[34]

In its subsequent decision, the ECtHR agreed, holding that,

> "an individual may, under certain conditions, claim to be the victim of a violation occasioned by the mere existence of secret measures or of legislation permitting secret measures, without having to allege that such measures were in fact applied to him."[35]

The ECtHR noted that to hold otherwise might reduce Article 8 to a "nullity," since a state could potentially violate a person's rights in secret, without any risk that a person could bring a claim

---

[33] European Convention for the Protection of Human Rights and Fundamental Freedoms, art. 8, Apr. 11, 1950, 213 U.N.T.S. 221 [hereinafter ECHR] (as amended), available at http://conventions.coe.int/Treaty/en/Treaties/Html/005.htm (entered into force Sept. 3, 1953).

[34] *Klass*, *supra* note 30, at para. 27; *cf.* Clapper v. Amnesty International USA, 133 S.Ct. 1138 (2013).

[35] *Id.* at para. 34.

for relief.[36] Thus, the ECtHR confirmed the Commission's decision on the admissibility of the application. Having determined the application admissible, the court addressed the threshold Article 8 question: whether the activity complained of constituted an interference with the applicant's "right to respect for his private and family life, his home and his correspondence."[37] The Court found that "the mere existence of the legislation" constituted a "menace" of surveillance which,

> "necessarily strikes at freedom of communication between users of the postal and telecommunication services and thereby constitutes an 'interference by a public authority' with the exercise of the applicants' right to respect for private and family life and for correspondence."[38]

The court then addressed whether the surveillance regime was otherwise justified. First, the Court found that, since the surveillance at issue had its basis in an Act of the German Parliament, it was done in "accordance with the law." Second, the Court also held, simply, that the aim of the surveillance was for legitimate purposes, namely, to protect national security and for the prevention of disorder or crime.[39] The more difficult question, according to the Court, was:

> "whether the means provided under the impugned legislation for the achievement of the above-mentioned aim remain in all respects within the bounds of what is necessary in a democratic society."[40]

The Court conceded that in extraordinary circumstances, legislation that provides for secret surveillance of physical or electronic communication can be "necessary in a democratic society."[41] In coming to this conclusion, the Court took judicial notice of the facts that surveillance technology was rapidly advancing and that European states did find themselves threatened by sophisticated terrorists.[42] As such, domestic legislatures should enjoy some, but not unlimited, discretion in outlining government surveillance powers.[43] However, because such laws pose a danger of "undermining or even destroying democracy on the ground of defending it," legislatures may not, simply "adopt whatever measures they deem appropriate" in their "struggle against espionage and terrorism."[44] Getting to the heart of whether such surveillance is

[36] *Id.* at para. 36.

[37] ECHR, art. 8, *supra* note 33.

[38] Klass, *supra* note 310, at para. 41.

[39] *Id.* at 46.

[40] *Id.* at 46.

[41] *Id.* at 48.

[42] Klass, *supra* note 310, at para. 48.

[43] *Id.* at 49.

[44] *Id.* at 49.

necessary in a democratic society, the court stated, "whatever system of surveillance is adopted, there [must] exist adequate and effective guarantees against abuse."[45]

The court concluded that the German law did not violate the applicants' Article 8 rights because the law limited the ability of the government to conduct surveillance, "to cases in which there are factual indications for suspecting a person of planning, committing or having committed certain serious criminal acts," and that, "Consequently, so-called exploratory or general surveillance is not permitted by the contested legislation."[46] This test has been largely adopted in subsequent ECtHR decisions, with some modifications (including more restrictive requirements when determining whether conduct is "in accordance with law") developing in a few important cases. The analysis below provides an overview of the court's reasoning and relevant case law, as announced in its most prominent subsequent cases.

Because of the secret nature of the surveillance at issue, the ECtHR has generally allowed applicants' standing, even without having to allege facts that would support a finding that the secret surveillance was actually applied to them.[47] In recent cases, the ECtHR continues to adhere to the finding announced in *Klass* that the mere existence of legislation allowing secret surveillance constitutes an interference with a person's Article 8 rights[48] – specifically "private life" and "correspondence."[49] In *Malone v. the United Kingdom*,[50] in 1984, the ECtHR reaffirmed this position, holding that because telephone conversations fell within the scope of "private life" and "communications," the existence of legislation that allowed the interception of telephone conversations amounted to an interference with the applicant's rights.[51] This extends to general programs of surveillance as well as targeted eavesdropping on private conversations.[52] Because of the essentially settled nature of this finding, most of the interesting judicial reasoning happens in answering the subsequent questions.

Initially, the requirement that an act of interference must be in accordance with the law was also easy to overcome. In *Klass*, the ECtHR held that since the surveillance at issue, the alleged interception of the applicants' telephone calls, had its basis in an Act of the German Parliament

[45] *Id.* at 50.

[46] *Id.* at 51.

[47] This was initially determined in *Klass*, *supra* note 30, but has been favorably cited and applied in recent cases as well; *see e.g. Iordachi*, *supra* note 30.

[48] The primary cases cited in ECtHR jurisprudence are *Klass*, *supra* note 30; *Malone*, *supra* note 30, at para 64; *Weber*, *supra* note 30, at paras. 77-79; *Ekimdzhiev*, *supra* note 30, at para 69; *Liberty*, *supra* note 30, at para 57; and *Iordachi*, *supra* note 30, at para 34. A number of other cases also recite this proposition.

[49] *Liberty*, *supra* note 30, at para 56; *Weber*, *supra* note 30, at para 77.

[50] *Malone*, *supra* note 30.

[51] *Id.* at para 64.

[52] *Liberty*, *supra* note 30, at para 63.

that specifically authorized such measures, it was done in accordance with the law.[53] However, in subsequent cases, the ECtHR has added additional tests to determine the answer to this question. By 1984, the *Malone* court recognized that this requirement also demanded more than just compliance with domestic law. Quoting from intervening judgments of the court, the *Malone* court stated,

> "Firstly, the law must be adequately accessible: the citizen must be able to have an indication that is adequate in the circumstances of the legal rules applicable to a given case. Secondly, a norm cannot be regarded as 'law' unless it is formulated with sufficient precision to enable the citizen to regulate his conduct: he must be able - if need be with appropriate advice - to foresee, to a degree that is reasonable in the circumstances, the consequences which a given action may entail."[54]

These requirements of accessibility, foreseeability and compatibility with the rule of law were announced in the *Malone* case, and have been reaffirmed in subsequent surveillance cases. At present, for an interference to be conducted in accordance with the law, as the Convention requires, the ECtHR must be satisfied that, as a threshold matter, the surveillance has some basis in domestic law. If it does, the Court then determines whether the "quality of the law" is sufficient; that is, 1) the enabling law must be "accessible to the person concerned," 2) the person must be able to foresee the consequences of the law for him- or herself,[55] and 3) the law itself must be compatible with the rule of law.[56]

In *Weber and Saravia v. Germany*,[57] the applicants claimed violations under the same German eavesdropping law that was at issue in *Klass*. Rather than taking issue with targeted interception of telecommunications of specific individuals, however, the applicants in the *Weber* case claimed that their Article 8 rights had been violated by a broader intelligence practice of "strategic monitoring" of telecommunications and the subsequent uses of such information (including information-sharing with other agencies).[58] In that case, the ECtHR found that the domestic courts had determined the surveillance at issue was covered by domestic law, and that, "the Court cannot question the national courts' interpretation except in the event of flagrant non-

---

[53] *Klass*, *supra* note 30, at para 43.

[54] *Malone*, *supra* note 30, at para 66, *quoting* Sunday Times v. United Kingdom, [1979] ECHR 1, at para 49; Silver and Others v. United Kingdom, [1983] ECHR 5, paras. 87-88.

[55] The most recent detailed elaboration of this requirement is in *Weber*, *supra* note 30, paras. 93-95; *see also Liberty*, *supra* note 30, at para 59-63; *Ekimzheiv*, *supra* note 30, at paras. 74-77.

[56] *See Weber*, *supra* note 30, at para 84, *citing* Kruslin v. France, [1990] ECHR 10, at para. 27 (1990); Huvig v. France, [1990] ECHR 9, at para 26 (1990); Lambert v. France, [1998] ECHR 75, at para. 23 (1998); Perry v. the United Kingdom, [2003] ECHR 375, at para. 45 (2003); *Ekimdzhiev*, *supra* note 30, at para. 71; *Liberty*, *supra* note 30, at para. 59; *see also Iordachi*, *supra* note 30, at para 37.

[57] *Weber*, *supra* note 30.

[58] *Id.* at para 4.

observance of, or arbitrariness in the application of, the domestic legislation in question."[59] In a number of other cases, the parties and the court simply accept that the surveillance at issue has the requisite basis upon a showing by the government that some relevant law exists.[60]

The "accessibility" and "foreseeability" requirements are often intertwined in the ECtHR's analysis, although sometimes the issue of accessibility is separated from the foreseeability inquiry, and is not given as much direct consideration by the Court.[61] In *Liberty v. the United Kingdom*, the applicant charity organization alleged that the UK Ministry of Defence operated a facility that was capable of intercepting 10,000 simultaneous telephone channels operating between Dublin to London and from London to the European Continent, as well as a certain amount of radio-based telephone, facsimile, and email communications carried between two British Telecom stations.[62] The government refused to confirm or deny the specific allegations, but agreed, for purposes of the litigation, that the applicants were of the category of legal persons who could be subject to having their communications intercepted by the government under its intelligence gathering programs.[63]

The government further claimed that revealing additional information about the specific arrangements authorized by the Secretary of State in relation to any warrants issued would compromise national security secrets.[64] They also refused to disclose the manuals and instructions which detailed the safeguards and arrangements put in place to govern the use of the program.[65] In their defense, the government stated that "the detailed arrangements were the subject of independent review by the successive Commissioners, who reported that they operated as robust safeguards for individuals' rights."[66]

Liberty argued that the secret nature of the Secretary's "arrangements" under the Interception of Communications Act rendered these procedures and safeguards inaccessible to the public and made it impossible for the public to foresee how and in what circumstances the government could intercept their communications.[67] The ECtHR agreed with the government's contentions that all the elements of the accessibility and foreseeability requirements did not need to be specified in primary legislation (for example, they could be specified in administrative orders

[59] *Id.* at para 90.

[60] For examples, see e.g. *Ekimdzhiev*, *supra* note 30, at para 72; *Iordachi*, *supra* note 30, at para 32; *Liberty*, *supra* note 30, at para 60.

[61] *See Ekimdzhiev*, *supra* note 30, at para 73; *Weber*, *supra* note 30, at para 92.

[62] *Liberty*, *supra* note 30, at para 5.

[63] *Id.* at para 47.

[64] *Id.* at para 48.

[65] *Id.*

[66] *Id.*

[67] *Id.* at para 60.

and other soft law sources), but that secondary sources could satisfy this requirement "only to 'the admittedly limited extent to which those concerned were made sufficiently aware of their contents.'"[68]

However, the ECtHR held that the government had violated the applicants' Article 8 rights in that case. The Court came to this conclusion for a few reasons. First, the accessible law did not place any restrictions on the type of external (non-UK) communications that could be included in a warrant, a fact that the Court found indicative of "virtually unfettered" executive discretion.[69] Second, the Act granted wide discretion to the authorities to determine which of the collected communications to actually review substantively. The Secretary of State could issue certificates describing material to be examined, using broad limiting terms and reasons such as "national security" to authorize review of the contents of communications.[70] These certificates could be applied to all communications except those "emanating from a particular address in the United Kingdom," unless the Secretary determined such interception was necessary to prevent or detect acts of terrorism.[71] The Act also required the Secretary to

> "make such arrangements as he consider[ed] necessary" to ensure that material not covered by the certificate was not examined and that material that was certified as requiring examination was disclosed and reproduced only to the extent necessary."[72]

Importantly, details of these arrangements were secret and not made accessible to the public.[73] A Commissioner did make annual reports stating that the Secretary's arrangements were in accordance with the law, but the ECtHR held that, while these reports were helpful, did not make the details of the scheme any more clear or accessible to the public, since the Commissioner was not allowed to reveal details about the arrangements in his public reports.[74] Indeed, the Court stated that,

> "the procedures to be followed for examining, using and storing intercepted material, inter alia, should be set out in a form which is open to public scrutiny and knowledge."[75]

---

[68] *Liberty*, *supra* note 30, at para 61, quoting *Malone*, *supra* note 30.

[69] *Id.* at para 64.

[70] *Id.* at para 65

[71] *Id.*

[72] *Id.* at para 66.

[73] *Id.*

[74] *Liberty*, *supra* note 30, at para 67.

[75] *Id.*

The ECtHR dismissed the government's claims that revealing such information publicly would damage the efficacy of the government's intelligence operations because, as indicated in its earlier decision in *Weber*, the German government had included such guidelines and restrictions in its primary (and publicly accessible) legislation itself.[76]

In conclusion, the court held that the domestic law did not "provide adequate protection against abuse of power" because of its broad scope and the "very wide discretion conferred on the State to intercept and examine external communications."[77] The Court found it particularly important that the government did not make its procedures for "examin[ing], sharing, storing and destroying intercepted material" accessible to the public.[78]

In *Weber*, the court also laid out these requirements in some detail. In that case, the Court stated that,

> "where a power vested in the executive is exercised in secret, the risks of arbitrariness are evident. It is therefore essential to have clear, detailed rules on interception of telephone conversations, especially as the technology available for use is continually becoming more sophisticated…. Moreover, since the implementation in practice of measures of secret surveillance of communications is not open to scrutiny by the individuals concerned or the public at large, it would be contrary to the rule of law for the legal discretion granted to the executive or to a judge to be expressed in terms of an unfettered power. Consequently, the law must indicate the scope of any such discretion conferred on the competent authorities and the manner of its exercise with sufficient clarity to give the individual adequate protection against arbitrary interference."[79]

In the case of *Iordachi and Others v. Moldova*,[80] the Court also found a violation of Article 8. In that case, the court found that the Moldovan law at issue lacked adequate clarity and detail because 1) there was no judicial control over the granting of applications for interceptions, 2) the law was very open-ended in regards to the persons potentially within its reach, and 3) the requirements for granting warrants were imprecise.[81] Even after the Moldovan government modified its law to provide for judicial approval of warrants and the definition of a general class

[76] *Id.* at para 68.

[77] *Id.* at para 69.

[78] *Id.* at para 69.

[79] *Weber*, *supra* note 30, at paras 93-95 (internal citations omitted). This language was also cited approvingly in *Liberty*, *supra* note 30.

[80] *Iordachi*, *supra* note 30.

[81] *Id.* at para 41.

of crimes subject to justify interception, the Court felt it had not gone far enough.[82] Additionally, the court stated that the legislation lacked precise details about how the government should screen gathered intelligence for useful information, preserve its integrity and confidentiality, and provide for its destruction.[83] Interestingly, the ECtHR also stated that the Moldovan secret surveillance system appeared "overused" since the courts approved "virtually all" of the prosecutor's requests for warrants. The court also noted that the numbers of issued warrants each year over a three-year period (2300, 1900, and 2500, respectively) was indicative of "inadequacy" in the "safeguards contained in the law."[84]

Additionally, under Article 8 jurisprudence, the law at issue must itself be compatible with the broader notion of the rule of law. In *Weber*, the ECtHR found that the German law in question did contain adequate safeguards against arbitrary interference.[85] In the *Ekimdzhiev*[86] case, the court found that a Bulgarian law provided sufficient safeguards, at the authorization stage, so that if it were "strictly adhered to" only specifically delineated forms of communications would be intercepted.[87] However, because the law did not provide for any independent review of the intelligence agency's implementation of these measures after the initial authorization stage, it failed to satisfy the requirement that it provide adequate guarantees against the risk of abuse.[88]

The ECtHR also found that, although the lack of provisions requiring notification to a person that their communications had been intercepted was not itself unreasonable, a blanket classification of information, in perpetuity, creates the untenable situation where,

> "unless they are subsequently prosecuted on the basis of the material gathered through covert surveillance, or unless there has been a leak of information, the persons concerned cannot learn whether they have ever been monitored and are accordingly unable to seek redress for unlawful interferences with their Article 8 rights."[89]

Finally, if a form of interference (e.g. surveillance) passes all the prior tests (meaning it is otherwise in "accordance with law"), it must still be "necessary in a democratic society" to achieve one or more legitimate aims spelled out in the Convention. In essence, this inquiry requires a finding of proportionality, and authorities maintain a "fairly wide margin" of

[82] *Id.* at paras 43-44.

[83] *Id.* at para 48.

[84] *Id.* at para 52.

[85] *Weber*, *supra* note 30, at para 101.

[86] *Ekimdzhiev*, *supra* note 30.

[87] *Id.* at para 84.

[88] *Id.* at para 93.

[89] *Id.* at para 91.

discretion, but such discretion is not unlimited.[90] Specifically, there must be adequate and effective guarantees to prevent abuse and, after a finding of proportionality (as the first step of this analysis), the court undertakes a holistic overall assessment (for safeguards against abuse), based on: all the facts of the case, the nature, scope and duration of the possible measures, the grounds required for ordering them, the authorities competent to authorize, carry out and supervise them, and the kind of remedy provided by the national law.[91]

In *Weber*, again analyzing the same German law that was at issue in *Klass* (as amended over the intervening years in subsequent cases), the Court's conclusion was not changed by the fact that in *Weber*, the applicants were complaining about broader strategic surveillance programs than those at issue in *Klass*. In *Weber*, the German government justified their continued surveillance programs on the basis that they were necessary to protect against international terrorism, specifically from threats from groups like Al-Qaida.[92] Only ten percent of telecommunications were potentially monitored, and the monitoring was limited to a limited number of specified countries.[93] The law also limited the ability of the government to monitor the telecommunications of ex-patriot Germans living abroad and the government could not request identifying information about persons unless their communications included certain catchwords.

On the other hand, the applicants complained that the law was overbroad and that no real geographic restrictions existed, that identification could occur more easily than the government admitted, and movements of persons using cellular phones could be tracked.[94] However, despite amendments that had broadened the scope of permissible surveillance under the law, the Court found that the law continued to meet the requirements imposed by ECtHR case law because many of the restrictive limitations on authorization, implementation and termination of surveillance continued to provide "considerable safeguards against abuse."[95] Similarly, the Court found that additional safeguards in the law rendered additional uses, transmissions, destruction, and sharing of collected information justified under the Convention.[96]

*b. THE UNITED STATES*

Mass communications surveillance by the U.S. Federal Government's intelligence and law enforcement agencies has been occurring for decades. Details about the BRUSA Circuit and the early UKUSA Agreement were classified until 2010 when the NSA finally declassified and

[90] *Weber*, *supra* note 30, at para 106.

[91] *Id.*

[92] *Id.* at para 109.

[93] *Id.* at para 110.

[94] *Id.* at para 111.

[95] *Weber*, *supra* note 30, at para 115-118.

[96] *See id.* at paras. 119-138.

revealed the early UKUSA documents[97] pursuant to an Executive Order signed by Bill Clinton fifteen years earlier.[98] In 1978, Congress enacted the Foreign Intelligence Surveillance Act (FISA)[99] to check and balance electronic government surveillance and individual rights to privacy under the Fourth Amendment to the U.S. Constitution.[100] FISA allows the government to intercept communications between U.S. citizens and foreign nationals (or those suspected of being foreign nationals), and to maintain secrecy about whose correspondence the government has intercepted. FISA established two courts, FISC and the Foreign Intelligence Surveillance Court of Review (FISCR), drawing upon Federal judges from Article III courts to administer secret, non-adversarial, proceedings initiated by government agencies to approve government requests to collect information under FISA. Notably, court proceedings and opinions are generally secret and not available for public scrutiny. Indeed, during the first 24 years of its existence, from its inception until 2002, the FISC only ever publicly released one single opinion (which did not relate to electronic surveillance) and, it turned out, had never rejected a government application to conduct surveillance.[101]

In 2002, the FISC, acting *en banc*, publicly released an opinion signed by all seven judges that refused to allow the government to use the USA PATRIOT Act to enable closer collaboration by intelligence agents and criminal prosecutors to prosecute crimes uncovered through foreign communications intelligence surveillance.[102] Six months later, the FISCR sharply overruled the FISC opinion, holding that the FISC had "not only misinterpreted and misapplied minimization procedures it was entitled to impose... [it] may well have exceeded the constitutional bounds that restrict an Article III court."[103] The FISCR also stated that maintaining a divide between criminal

---

[97] The United States National Security Agency released declassified documents related to the early UKUSA agreement on its website at http://www.nsa.gov/public_info/declass/ukusa.shtml; the early papers, including the initial request from the British Embassy proposing the information sharing arrangement, can be found in Early Papers Concerning US-UK Agreement – 1940–1944, available at http://www.nsa.gov/public_info/_files/ukusa/early_papers_1940-1944.pdf.

[98] Executive Order 12958—Classified National Security Information (as amended), *available at* http://www.fas.org/sgp/clinton/eo12958.pdf.

[99] Foreign Intelligence Surveillance Act, Pub. L. No. 95-511, 92 Stat. 1783 (codified as amended at 50 U.S.C. §§ 1801-1811 (2002); 18 U.S.C. §§ 2511, 2518-19 (2002)).

[100] Diane Carraway Piette and Jesslyn Radack, *Piercing the Historical Mists: The People and Events behind the Passage of FISA and the Creation of the Wall*, 17 Stan. L. & Pol'y Rev. 437, 438-439 (2006). FISA was enacted after the Supreme Court's 1972 decision in *United States v. United States Dist. Court for Eastern Dist. of Mich.* (the "Keith" decision) (1972), in which the Court suggested that the Constitutional framework applicable to national security cases might be different than in cases dealing with the "surveillance of 'ordinary crime.'" Clapper v. Amnesty International USA, 133 S.Ct. 1138, 1143, *quoting* Keith, at 322-23).

[101] Piette and Radack, *supra* note 100, at 439. The first publicly released opinion *In re Application of United States for an Order Authorizing the Physical Search of Nonresidential Premises and Personal Property* (FISC June 11, 1981), reprinted in S. Rep. No. 97-280, *available at* http://www.intelligence.senate.gov/pdfs97th/97280.pdf (finding the FISC did not have statutory authority to approve warrants for physical searches).

[102] *Id.*

[103] *In re* Sealed Case No. 02-001, 310 F.3d 717, 731 (FISA Ct. Rev. 2002).

and intelligence investigations that walled off certain investigatory and prosecutorial collaboration "was never required and was never intended by Congress."[104] In the intervening years, a number of lawsuits have emerged challenging government powers under FISA and its amending legislation, including the Foreign Intelligence Surveillance Amendments Act (FISA Amendments Act)[105] and the USA PATRIOT Act.[106] The purpose of this section is not necessarily to document each and every case, but rather to explore the judicial reasoning that pervades these decisions.

In February 2013, the United States Supreme Court decided *Clapper v. Amnesty International USA*,[107] which stands in fairly sharp contrast to the line of ECtHR cases beginning with *Klass*, as discussed above. In *Clapper*, the Court rejected a challenge to the constitutionality of FISA mounted by a number of attorneys and a variety of other human rights, legal, media, and labor organizations. In that case, the plaintiffs sued the United States government, claiming that surveillance authorized under Section 1881a (otherwise known as Section 702; enacted in 2008 by the FISA Amendments Act) violated their Constitutional rights. The organizations claimed, similarly to the attorney's in *Klass*, that, because of their regular communications with overseas persons, there was an "objectively reasonable likelihood that their communications will be acquired under section 1881a at some point in the future," and that the threat of this this acquisition had caused them to take costly preventative measures aimed at preserving the confidentiality of their communications.[108]

Despite the fact that, due to the law's secrecy requirements, the government is the only entity that knows which communications have been intercepted, the Court held that third-parties like Amnesty International do not have standing to challenge the Act because they cannot show that they have been harmed[109] (precisely because they don't have access to information about the government's surveillance activities). Unlike at the ECtHR, the Supreme Court held that the mere existence of secret surveillance did not grant standing, effectively blocking any challenge to secret programs absent some form of prior disclosure.

Enter Edward Snowden.

---

[104] Neil A. Lewis, *Court Overturns Limits on Wiretaps to Combat Terror,* N.Y. TIMES, Nov. 19, 2002, at Al; Piette & Radack, *supra* note 1000, at 440.

[105] Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008, H.R. 6304.

[106] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (USA PATRIOT Act) of 2001, Pub. L. No. 107-56, 115 Stat. 272 (codified in scattered sections of the U.S.C.) (hereinafter the "PATRIOT Act").

[107] Clapper v. Amnesty International USA, 133 S.Ct. 1138 (2013).

[108] *Id.* at 1143.

[109] *Id.* at 1155.

Interestingly, and perhaps not by coincidence, Snowden's first disclosure of classified NSA documents related to the law at issue in *Clapper*, section 1881a. In May 2013, Snowden leaked a secret FISC order[110] (the Verizon Order) to Guardian journalist Glenn Greenwald (which was published on June 5). In that order, the FISC directed Verizon, one of the largest telecommunications providers in the United States, to turn over phone call metadata on millions of Americas to the NSA on an on-going and daily basis.[111] Justice Claire Egan's decision, released September 17, 2013, upheld a subsequent order requiring similar, continued compliance by an unnamed telecommunications provider.[112] Following the Guardian's publication of the Verizon Order, the American Civil Liberties Union (ACLU) and New York Civil Liberties Union (NYCLU) filed a lawsuit against the NSA.[113] Both the ACLU and NYCLU claimed standing in their complaint because they were actually Verizon customers during the dates covered by the FISC order.[114]

In 2006, the Electronic Frontier Foundation (EFF) sued At&T for violating its customers privacy by collaborating with the NSA to conduct electronic surveillance of its customers.[115] In response to this case, and dozens of other lawsuits fueled by news reports of the government's warrantless surveillance program, Congress enacted Section 802 of the FISA Amendments Act to grant these corporations retroactive immunity.[116] Subsequently, in 2008, EFF filed suit against the NSA and various other federal entities in *Jewel v. NSA*[117] claiming that the same warrantless dragnet surveillance program violated the plaintiffs' Constitutional rights.[118] Although this case was based on leaked documentation of the alleged practices, unlike *Clapper*, the case was also originally dismissed on standing grounds.[119] However, the Ninth Circuit later reversed and allowed the plaintiffs standing to continue their suit.[120] Most recently, in July 2013, the U.S.

---

[110] A copy of the order is available on the Guardian's website at http://www.guardian.co.uk/world/interactive/2013/jun/06/verizon-telephone-data-court-order.

[111] Glenn Greenwald, *NSA collecting phone records of millions of Verizon customers daily*, The Guardian, June 6, 2013 (originally published on June 5, 2013), available at http://www.guardian.co.uk/world/2013/jun/06/nsa-phone-records-verizon-court-order/.

[112] Egan Opinion, *supra* note 22.

[113] E. Nakashima, E. & S. Wilson, *ACLU sues over NSA surveillance program*, The Washington Post, June 11, 2013, *available at* http://articles.washingtonpost.com/2013-06-11/politics/39893547_1_surveillance-program-clapper-jr-aclu/.

[114] ACLU Complaint, American Civil Liberties Union v. Clapper, case no. 13 Civ. 3994, filed June 11, 2013, in the U.S. District Court for the Southern District of New York, *available at* https://www.aclu.org/files/assets/nsa_phone_spying_complaint.pdf.

[115] NSA Telecomms. Records Litig. v. AT&T Corp., 671 F.3d 881, 890-91 (9th Cir. 2011).

[116] *Id.* at 891-92.

[117] Jewel v. NSA, 2013 U.S. Dist. LEXIS 103009 (N.D. Cal., July 23, 2013).

[118] *Id.* at *9-*11.

[119] Jewel v. NSA, 2010 U.S. Dist. LEXIS 5110 (N.D. Cal., Jan. 21, 2010).

[120] Jewel v. NSA, 673 F.3d 902 (9th Cir. Cal., 2011).

District Court for the Northern District of California rejected the government's state secrets defense, allowing the plaintiff's First and Fourth Amendment claims to move forward.[121] The District Court did, however, conclude that the plaintiff's might have an uphill battle to overcome standing after *Clapper*:

> "Although the Court finds, at this procedural posture, that Plaintiffs here do not allege the attenuated facts of future harm which barred standing in Clapper, the potential risk to national security may still be too great to pursue confirmation of the existence or facts relating to the scope of the alleged governmental Program."[122]

Similarly, in *CCR v. Obama*, the Ninth Circuit affirmed dismissal of a case challenging the Terrorist Surveillance Program, which ended in 2007.[123] The Court found that the plaintiffs lacked standing, much like the plaintiffs in *Clapper*,

> "Although CCR might have a slightly stronger basis for fearing interception because of the lack of FISC involvement, CCR's asserted injury relies on a different uncertainty not present in [*Clapper*], namely, that the government retained 'records' from any past surveillance it conducted under the now-defunct TSP. In sum, CCR's claim of injury is largely factually indistinguishable from, and at least as speculative as, the claim rejected in [*Clapper*]."[124]

These cases are far from the only challenges mounted by civil liberties organizations against government programs that mandated high levels of information secrecy. In just one additional example, although not a secret surveillance case *per se*, a Federal District Court judge held, in January 2013, that the United States government could keep information about its "targeted killing program" a secret.[125] In that case, the ACLU and New York Times had filed Freedom of Information Act lawsuits against the Department of Justice seeking information about the contested killing program. In her decision, Judge MacMahon stated that:

> "The FOIA requests here in issue implicate serious issues about the limits on the power of the Executive Branch under the Constitution and laws of the United States, and about whether we are indeed a nation of laws, not of men…. However… I can find no way around the thicket of laws and precedents that effectively allow the Executive Branch of our Government to proclaim as

[121] Jewel v. NSA, 2012 U.S. Dist. LEXIS 176263 (N.D. Cal., Dec. 12, 2012), *as amended by* Jewel, *supra* note 117.

[122] Jewel, *supra* note 117, at *54.

[123] In Re NSA Telecomms. Records Litig. (CCR) v. Obama, 2013 U.S. App. LEXIS 11630 (9th Cir., 2013).

[124] *Id.* at *3-4.

[125] New York Times Co., v. U.S. Dept. of Justice, 2013 WL 50209 (S.D.N.Y., 2013).

> perfectly lawful certain actions that seem on their face incompatible with our Constitution and laws, while keeping the reasons for its conclusion a secret."[126]

These cases demonstrate that U.S. courts are exercising restraint when confronting challenges to the federal government's claims of secrecy in the name of national security. This restraint is in fairly sharp contrast to the willingness of the ECtHR to allow challenges and hold governments accountable for secret surveillance.

These situations clearly represent the nature and existence of potentially dominating activity by the state and, as elaborated in the overall argument advanced in this paper, because the holdings effectively immunize the federal government from citizen review of the procedures and substance of government action they are highly suspect and problematic. In the very moments when these courts have been perfectly positioned to reduce government domination and protect the peoples' liberty, they have chosen to turn a blind eye or have a least been unwilling to robustly defend the Constitutional rights of American citizens.

## V. LIBERTY: INTERFERENCE OF DOMINATION?

### *a. LIBERAL LIBERTY: BERLIN'S NEGATIVE CONCEPTION OF FREEDOM*

Perhaps the most seminal essay in modern political philosophy on the topic of political liberty is Isaiah Berlin's *Two Concepts of Liberty*.[127] In that essay, Berlin outlines the trajectory of two different conceptions of liberty, what he calls "negative" and "positive" liberties. On one hand, negative liberty "is simply the area within which a [person] can act unobstructed by others."[128] A person's *degree* of freedom rests on whether, or how thoroughly, that person is prevented from doing something by another person.[129] A certain level of interference by another with one person's freedom to do something, in Berlin's view, can equate to coercion or slavery, and thus ought to be avoided.[130] On the other hand, Berlin defines positive liberty as a form of self-mastery; to have one's decisions depend on no other person or any other force.[131] Despite some claims that this distinction (sometimes referred to as "freedom from" and freedom to") doesn't

[126] Id. at *1.

[127] ISAIAH BERLIN, *Two Concepts of Liberty*, in LIBERTY: FOUR ESSAYS ON LIBERTY (Henry Hardy ed., Oxford University Press, 2d ed., 2002). For support of this claim, see ADAM SWIFT, POLITICAL PHILOSOPHY: A BEGINNER'S GUIDE FOR STUDENTS AND POLITICIANS 51 (2d rev. ed., Polity, 2006).

[128] BERLIN, *id.* at 169.

[129] *Id.*

[130] *Id.*

[131] *Id.* at 178.

hold up,[132] Berlin provides an insightful tracing of the use of positive ideas about liberty that informed the development of totalitarian regimes like the Nazis and former USSR.[133]

Berlin's conception of negative liberty, however, has provided the basis for much contemporary work on philosophical liberty in the liberal tradition. Berlin himself noted that his version of negative liberty was not "logically… connected with democracy or self-government," although democratic self-government may admittedly guarantee liberty better than other forms of rule.[134] "The answer to the question 'Who governs me?'", Berlin states, "is logically distinct from the question 'How far does the government interfere with me?'"[135] Other writers have distinguished between "effective freedom" and "formal freedom," as a way to clarify Berlin's distinctions between positive and negative and to make the point that the absence of restraint (defined in terms of *legal* restraints) does not always guarantee the actual ability of and individual to do something he or she is legally entitled to do (for example, a person may not be able to take an expensive international vacation because of economic hardship).[136] On one hand, negative freedom is concerned with the absence of state restraint (or interference), while positive freedom is concerned about equalizing the effective freedoms of everyone is a society (e.g. international vacations might be assured by a state mandating a certain level of basic income). Some forms of positive freedom might also privilege the value of political engagement and self-government, as opposed to viewing laws as an interference (whether justified or not) on personal liberty.[137]

### *b. NEO-REPUBLICAN LIBERTY: PETTIT'S THEORY OF NON-DOMINATION*

In recent decades, republicanism, as an alternative to liberalism, has received renewed attention. Philip Pettit, a champion of one form of republicanism, often termed neo-republicanism or civic-republicanism, proposes a conceptualization of freedom as the opposite of "defenseless susceptibility to interference by another" – or put more simply, non-domination or "antipower."[138] This proposition is part of a larger neo-republican research agenda based on

[132] *See* SWIFT, *supra* note 127, at 52-54.

[133] *See generally* Berlin, *supra* note 127; *see also* SWIFT, *supra* note 127, at 51.

[134] Berlin, *supra* note 127, at 177.

[135] *Id.*

[136] *See e.g.* SWIFT, *supra* note 127, at 55.

[137] *See id.* at 64.

[138] Philip Pettit, *Freedom as Antipower*, 106 Ethics 576, 576-77 (1996); Philip Petti, *Republican Freedom and Contestatory Democratization*, in I. Shapiro & C. Hacker-Cordon (eds.), DEMOCRACY'S VALUE, p. 165 (Cambridge University Press, 1999). *Cf.* PHILIP PETTIT, *REPUBLICANISM: A THEORY OF FREEDOM AND GOVERNMENT*, (Clarendon Press, 1997); PHILIP PETTIT, A THEORY OF FREEDOM: FROM THE PSYCHOLOGY TO THE POLITICS OF AGENCY (Oxford University Press, 2001); Philip Pettit, *Keeping Republican Freedom Simple: On a Difference with Quentin Skinner*, 30 Political Theory 339 (2002); Philip Pettit, *Agency-Freedom and Option-Freedom*, 15 Journal of Theoretical Politics 387 (2003); Philip Pettit, *Freedom and Probability: A Comment on Goodin and Jackson*, 36 Philosophy and Public Affairs 206 (2008); Philip Pettit, *The Instability of Freedom as Noninterference: The Case of*

three primary tenants: individual freedom (conceptualized as freedom as nondomination), limited government power over its citizens based on a mixture of constitutionalism and the rule of law (with an emphasis on the importance of the free state promoting the freedom of its citizens without dominating them), and a vigilant commitment by citizens to preserve the freedom preserving structure and substance of their government through active democratic participation.[139]

Contrary to Berlin's account of negative liberty – that a person is free to the extent that no other entity actually interferes with that person's activity – Pettit's neo-republican position does away with the requirement of actual interference, focusing on eliminating the danger (or potential danger) of arbitrary interference from others.[140] Rather than predicating freedom on ideas of self-mastery, autonomy, or a person's ability to act in accordance with their higher-order desires, an account of Berlin's positive liberty, neo-republican theory is more concerned with ensuring the ability of the people to self-govern, by reducing domination and arbitrary interference.[141]

Pettit's bases his account on the idea that the opposite of freedom is slavery (or the subjugation to arbitrary exercise of power).[142] Pettit is concerned that a conception of liberty limited to noninterference restricts our potential for appropriate emancipation from domination. Additionally, the noninterference view problematizes the application of law, as even generally freedom preserving restrictions built into the rule of law constitute interference with absolute liberty (for example, the penalization of premeditated murder).

According to its proponents, this neo-republican political theory owes its origins to the experiences of the early Roman republic, and has been influenced and adopted by early figures such as Machiavelli, Jefferson, and Madison, and, more recently, by writers like Quentin Skinner and Philip Pettit,[143] although the precise historiography is still somewhat controversial.[144] Frank

---

*Isaiah Berlin*, 121 Ethics 693 (2011); PHILIP PETTIT, ON THE PEOPLE'S TERMS: A REPUBLICAN THEORY AND MODEL OF DEMOCRACY (Cambridge University Press, 2012).

[139] Frank Lovett and Philip Pettit, *Neorepublicanism: A Normative and Institutional Research Program*, 12 Annual Review of Political Science 11 (2009).

[140] Frank Lovett, *Republicanism*, THE STANFORD ENCYCLOPEDIA OF PHILOSOPHY (Spring 2013 Edition), at § 3.2, Edward N. Zalta (ed.) (2013), at http://plato.stanford.edu/archives/spr2013/entries/republicanism/.

[141] *Id.*

[142] *See* Pettit, Antipower, *supra* note 13838; Lovett, *supra* note 1400, at § 1.2.

[143] Lovett, *supra* note 1400, at § 3.1; Quentin Skinner, LIBERTY BEFORE LIBERALISM (Cambridge University Press, 1998); Quentin Skinner, *The republican ideal of political liberty*, in G. Bock, Q. Skinner, & M. Viroli (eds.), MACHIAVELLI AND REPUBLICANISM, pp. 239-309 (Cambridge University Press, 1998); *see also* Z.S. Fink, THE CLASSICAL REPUBLICANS: AN ESSAY IN THE RECOVERY OF A PATTERN OF THOUGHT IN SEVENTEENTH CENTURY ENGLAND (Northwestern University Press, 1945); C. Robbins, THE EIGHTEENTH-CENTURY COMMONWEALTHMAN (Harvard University Press, 1959); J.G.A. Pocock, THE MACHIAVELLIAN MOMENT: FLORENTINE POLITICAL THOUGHT AND THE ATLANTIC REPUBLICAN TRADITION (Princeton University Press, 1979); M.N.S. Sellers, AMERICAN REPUBLICANISM: ROMAN IDEOLOGY IN THE UNITED STATES CONSTITUTION (New York University Press, 1994).

Lovett and Philip Pettit argue that their version of neo-republicanism has been adapted from what has been called "classical" republicanism to distinguish it from other, more communitarian, approaches.[145] Lovett also states that since political liberty ought to be "understood as a sort of structural relationship that exists between persons or groups, rather than as a contingent outcome of that structure," freedom is properly seen "as a sort of structural independence—as the condition of not being subject to the arbitrary power of a master."[146]

On another account, critical of Pettit's emphasis on nondomination as the core ethical-political commitment of republicanism itself, "domination should be seen as the expression of oligarchic (and even tyrannical) concentrations of power within society as a whole, as pathological results of a badly arranged society."[147] On this account, we should be concerned not only with limiting the arbitrary domination of some, and:

> "the emphasis should be placed on the ways in which the freedom of individual agents is rooted in the structure of social power as a whole: in ensuring that society is arranged in such a way as to orient social power not only negatively, but positively as well."[148]

Thus, power and domination are built into the structure of social institutions, and this structure, if constructed improperly, potentially allows institutions to dominate and subjugate the people systemically. This, in turn, makes it difficult for "individuals and groups to possess political control over the institutions which govern their lives," a serious problem for republican politics.[149] Domination, then, can become institutionalized and integrated into our social and political institutions in a way that creates systemic domination,[150] as well as evidenced in the relationships between agents of government and individuals or groups of citizens.

But what exactly is domination, from the neo-republican position? Domination requires the capacity to interfere, with impunity and in an arbitrary fashion, with certain choices that the dominated agent otherwise has the capacity to make (here, "certain" means that the scope of the interference need not impinge on all of the dominated agent's choices, but may be limited to certain choices of varying centrality or importance). Interference requires "an intentional

---

[144] Lovett, *supra* note 1400, at § 1.

[145] *See generally* Lovett and Pettit, *supra* note 13939.

[146] Lovett, *supra* note 1400, at § 1.2.

[147] Michael J. Thompson, *Reconstructing republican freedom: A critique of the neo-republican concept of freedom as non-domination*, 39 Philosophy Social Criticism 277, 278 (2013).

[148] *Id.*

[149] *Id.* at 279.

[150] Id. at 290.

attempt to worsen an agent's situation of choice."[151] Unintentional or accidental interference is not freely exercised subjugation. However, interference does encompass a wide amount of possible actions, including restraint, obstruction, coercion, punishment (or threat of punishment), and manipulation (which includes, in Pettit's view, "agenda fixing, the deceptive… shaping of people's beliefs or desires, [and] rigging… the consequences of people's actions").[152]

Thus, this sort of interference worsens the dominated agent's position – and causes damage – because it changes the options available to the person or alters the payoffs of the person's choices by allowing the subjugator to manipulate the options and payoffs in play. In this sense, the power-wielding agent has the necessary capacity to interfere. The agent must also be capable of interfering with impunity and at will (or arbitrarily) in order to fully dominate the other. This condition requires that the agent act without risk of penalty for interfering – whether from the victim themselves (directly or indirectly) or society at large. If these criteria are satisfied, then the agent has "absolutely arbitrary power."[153] The only check on the exercise of such power is in the agent itself – in that agent's free and capricious will. Thus, it follows that a person (X) is dominated by another (Y) when X has no legal recourse to contest actions by Y that interfere with X's situation of choice. Thus, because widespread state surveillance of the communications of its citizens has the potential to interfere with individual citizens' situations of choice (for example, by chilling free expression), this relationship exhibits domination.

In response to this conception of domination as the antithesis of liberty, the neo-republican project places a great premium on emancipation – through balancing power and limiting arbitrary discretion – and active political participation. Importantly, reversing roles would not solve the problem of domination, but would merely relocate it.[154] Fairly allocating power to both sides, on the other hand, does not just merely equalize the subjugation; if both sides – say the people and their government – may interfere with the other's affairs, then neither may act with impunity since the other may exact something in return.[155] Thus, "neither dominates the other."[156] This is an exemplification of what Pettit terms "antipower."[157] According to Pettit, "Antipower is what comes into being as the power of some over others – the power of some over others in the sense associated with domination – is actively reduced and eliminated."[158] Antipower, then, subjugates power and, as a form of power itself, allows persons to control the

[151] Pettit, Antipower, *supra* note 13838, at 578.

[152] *Id.* at 579.

[153] *Id.* at 580.

[154] *Id.* at 588.

[155] *Id.*

[156] *Id.*

[157] *See generally* Pettit, Antipower, *supra* note 13838.

[158] *Id.* at 588.

nature of their own destiny.[159] In this sense, the "person enjoys the noninterference resiliently" because they are not dependent on the arbitrary use of power, precisely because they have the power to "command noninterference."[160]

One way to provide a citizenry with the power to command noninterference is to regulate the resources of the powerful, which might include checks on and separations of power, regular representative elections, democratic participation, limited tenure of government officials, access to independent courts or other bodies with powers to review government action, and open access to information.[161] Because access to information is a prerequisite to seeking legal recourse for potentially dominating activities of another, this aspect of power regulation should take an important place in our domestic and international information policies.

Of course, as Pettit's neo-republican project concedes, fully eliminating domination may not be always be easy, or even completely possible, and antipower may exist to varying degrees. Commanding noninterference may require collective action, and this theory admittedly relies on the presence of institutions as means to administer government and facilitate the peoples' claims. This does not mean, however, that we ought to be complacent, or even limit our concern to reducing actual interference. On the contrary, if an act or policy of an institution or agent of government arbitrarily dominates the will and autonomy of citizens, thus violating their ability to self-govern, then these acts or policies and are unjustified and ought to be corrected.

Thus, under this neo-republican conception of liberty, the proposition that governments must allow their citizens enough access to information necessary for individual self-government is entirely appropriate. To be fully non-arbitrary and non-dominating, government must also respect and provide effective institutional and legal mechanisms for their citizenry to effectuate self-government and command noninterference. Establishing liberal access rights to information about government conduct and mechanisms that ensure that citizens can effectively command noninterference are justified on the grounds that they reduce the possibility of arbitrary, and actual, interference with the right of the people govern themselves. Such measures would also limit the institutionalization of systemic domination within political and social institutions, as Thompson fears.[162]

[159] *Id.* at 589.

[160] *Id.*

[161] *Id.* at 591.

[162] *See* Thompson, *supra* note 1477.

## VI. CONCLUSION

Government surveillance can be detrimental to individual liberty.[163] It may chill the exercise of civil liberties, such as free speech,[164] or may violate subjective and/or objective expectations of privacy that ought to be protected under the Fourth Amendment. Secret surveillance laws pose a danger of "undermining or even destroying democracy on the ground of defending it" in their "struggle against espionage and terrorism."[165] In the aggregate, databases of personal information provide the government with the opportunity to conduct longitudinal analysis of individual citizens' behavior and communication practices, and may result in sophisticated statistical analysis, including the forecasting of future action based on past events.

On Berlin's negative account of liberty, a person if free if she does not actually suffer interference: if she is not subjected to manipulation, coercion, threat, or compulsion. This view is indeed attractive. Can we really say that a person is less free to express themselves when no one ever actually interferes with their speech (despite the possibility, however vague and unlikely) than when no one *can* interfere at all? The noninterference view of freedom has been embraced by some, like Hobbes, Paley, and Bentham, to argue that that all law and every form of government restricts liberty.[166]

On the other hand, viewing freedom as antipower – as the absence of domination by another – allows us to respect the importance of noninterference in many cases, but also recognizes that the nonvoluntaristic rule of law (with opportunities for effective appeal and democratic participation) actually protects and preserves our freedoms, rather than restricting them as a means to some other end. A person living under a friendly despot is not in the same position – in terms of freedom – as the person living in a properly constituted constitutional democracy with limits on domination. Fully realizing a situation of more equalized reciprocal surveillance and rights to access and document information about government activities (with temporary exceptions as may be needed to protect national security) would give citizens greater ability to ensure their government was not overreaching and abusing its authority, to hold the state and state actors accountable for rights violations, and to maintain government as an entity that protects it citizens' freedoms without coming to subjugate them to arbitrary exercises of power.

Strict limitations on standing in cases challenging secret government surveillance activities constitute an interference with individual freedom, as the ECtHR has held.[167] The stark

---

[163] *See* Forcese and Freeman, *supra* note 1; Neil Richards, *The Dangers of Surveillance*, 126 Harvard L. Rev. 1934, 1934-35 (2013).

[164] Richards, *supra* note 163, at 1935.

[165] *Id.* at 49.

[166] Pettit, Antipower, *supra* note 13838, at 598-600; Lovett and Pettit, *supra* note 13939, at 13-15.

[167] *Id.*

differences in the ability of plaintiffs to claim violations of their Constitutional or basic human rights in the U.S. and at the ECtHR, provides a suggestive critique of the nature of the current judicial politics of surveillance and transparency in domestic U.S. courts. The unwillingness of U.S. courts to allow challenges to secret government surveillance programs on standing grounds is a failure of the judicial system to check the ability of the executive to usurp arbitrary domination over the people. It is a failure of antipower in America.

The primary point of this argument, then, is not that we eliminate or unduly restrict to ability of government and law enforcement to conduct surveillance (or to restrict access to certain information in some cases), but rather that we recognize the bargain we have struck, in our representative democratic society, that the government assume some surveillance powers – and thus encroach on our individual negative freedoms to some degree – because they have the ability (and the responsibility) to use these powers for the public good. Our contract, and our consent, does not negate the possibility of domination or the relevance of freedom.[168] However, this power cannot be granted without strings attached.

Information can (and does) provide and facilitate power. Significantly, the collection and use of large amounts of information (including communications metadata) can significantly impact the relationships between governments and their citizens.[169] Because access to information is often a prerequisite to exercising power or seeking redress for potential rights violations stemming from secret activities of others,[170] we must allow challenges to secrecy in government that tip the balance of information access to far too one side. An imbalance in information access between a people and their government will tip the scales of power and limit the ability of the people to exercise democratic oversight and control those they have put in power to represent them.[171] Freedom of information laws provide one way to access to government records and serve as a powerful and effective means for empowering oversight by journalists and ordinary citizens. These laws, which provide a legal mechanism for citizen-initiated reciprocal-surveillance must capture more information about the legal bases and secret surveillance programs to ensure that "adequate and effective guarantees against abuse"[172] exist. This form of reciprocal surveillance will grant citizens greater power to check government abuse and force even greater transparency.[173] Otherwise, our privacy and liberty risk becoming a "nullity."[174] The violation of our rights should not hinge on our *awareness* of government overreaching, but whether the

[168] Pettit, Antipower, *supra* note 13838, at 585.

[169] *See* Forcese and Freeman, *supra* note 1, at 481-84.

[170] *Id.*

[171] *Id.*

[172] Klass, *supra* note 310, at para. 50.

[173] Brin, supra note 6; Haggarty and Ericson, *supra* note 6, at 10.

[174] *Klass*, *supra* note 30, at para. 36.

government has in fact acted impermissibly, visibly or in secret. As such, our access to remedies (and information) should not similarly be limited solely to cases involving non-secret government action.

To preserve our freedom, we must also act to ensure our freedoms are protected; we must use the channels of democratic participation available to us to effectuate our own nondomination. These channels might include political participation, litigation, exercising our free speech rights, or documenting government conduct in various ways, such as through filming public officials exercising their public duties in public spaces or filing freedom of information requests to uncover suspected wrongdoing. We should not be forced to grant our government the ability to exercise its powers arbitrarily, without oversight, especially when those powers have the ability to limit our freedoms. Implementing and maintaining greater checks on the exercise of government surveillance powers would remove the opportunity for subjugation, enable an important emancipation from information secrecy, and promote individual liberty.

###

Preliminary Draft – Please Do Not Cite Without Permission
To be Published in *I/S: A Journal of Law and Policy for the Information Society*
9 ISJLP ___ (2014).
http://www.is-journal.org

# DOMESTICATING PROGRAMMATIC SURVEILLANCE: SOME THOUGHTS ON THE NSA CONTROVERSY

Nathan Alexander Sales*

On June 14, 2003, a Jordanian man named Ra'ed al-Banna landed at Chicago's O'Hare international airport after a long flight from Amsterdam.[1] His paperwork was in perfect order: He held a legitimate Jordanian passport, he'd obtained a visa authorizing him to work in the United States, and he'd previously visited this country without incident. Nevertheless, al-Banna was pulled aside for a little extra scrutiny at the O'Hare customs checkpoint. He'd been flagged by an automated system that national security officials use to analyze huge troves of airline passenger reservation data, which carriers must provide when flying to the United States.[2] The officers who questioned him found him evasive, so they refused him entry and put him on the next flight home.

A year and a half later, a massive car bomb detonated in Hilla, Iraq, killing 132 police recruits. At the time, it was the deadliest suicide bombing Iraq had seen. "The driver was Ra'ed al-Banna. We know that because when authorities found the steering wheel of his car, his forearm was still chained to it."[3] It's impossible to know whether al-Banna would have mounted a similar attack in the United States if he hadn't been turned away at the border. But we're fortunate not to have found out.

The recently disclosed NSA efforts to collect vast amounts of telecommunications information involve a different agency and different data. But they aim at the same objective—detecting nascent threats before they can do harm—and raise the same vital questions about how to balance the competing demands of national security on the one hand and privacy and civil liberties on the other. This Essay uses the NSA programs as a vehicle for thinking more broadly about programmatic surveillance—the collection of large amounts of data in an attempt to identify yet-unknown terrorists, spies, and other threats. It begins by addressing the potential national security benefits of bulk data collection. It then proposes some guiding principles to help ensure that any such surveillance is consistent with basic privacy and civil liberties values. It concludes by offering some preliminary thoughts on how well the NSA programs comport with these first principles and, where they fall short, how to modify them. The constitutional and statutory issues raised by the programs have been ably addressed elsewhere,[4] including by other



---

* Assistant Professor of Law, George Mason University School of Law. This Essay is based on a statement prepared for a June 9, 2013 workshop of the Privacy and Civil Liberties Oversight Board.

[1] *See* Stewart A. Baker & Nathan Alexander Sales, *Homeland Security, Information Policy, and the Transatlantic Alliance*, *in* LEGAL ISSUES IN THE STRUGGLE AGAINST TERROR 277, 277-78 (John Norton Moore & Robert F. Turner eds. 2010).

[2] 49 U.S.C. § 44909(c)(2), (3).

[3] Baker & Sales, *supra* note 1, at 278.

[4] *Compare, e.g.*, Oversight of the Administration's use of FISA Authorities, Hearing Before the H. Comm. on the Judiciary, 113d Cong. (2013) (statement of Steven G. Bradbury, Dechert LLP), *with id*. (statement of Jameel Jaffer, ACLU).

participants in this symposium; my contribution will focus more on the policy considerations than the legal ones.

I.

Based on press accounts, the recently revealed NSA activities appear to involve a technique called *programmatic*, or *bulk*, surveillance.[5]

The first initiative—the so-called *telephony metadata* or *section 215* program—reportedly involves the use of orders issued by the FISA court pursuant to section 215 of the USA PATRIOT Act[6] to collect transactional information about every telephone call placed over Verizon's network (e.g., numbers dialed and call duration, but not content or location data), and probably the networks of other carriers as well.[7] At the risk of understatement, that is a monumental amount of data. Once collected, these records are warehoused in vast government databases and made available to intelligence analysts in narrow circumstances: The FISA court's order is said to allow analysts to query the databases only if there is "reasonable suspicion, based on specific articulable facts, that a particular telephone number is associated with specified foreign terrorist organizations."[8] It appears that the NSA, not the FISA court, is responsible for determining whether the requisite reasonable suspicion is present in a given case. In 2012, analysts apparently looked at the records of some 300 users.[9] The FISA court has upheld the program on both constitutional grounds (concluding that the acquisition of bulk telephony metadata was not a "search" within the meaning of the Fourth Amendment, largely on the strength of the third-party doctrine recognized in *Smith v. Maryland*[10]) and statutory ones (concluding that troves of data sought were tangible things that are relevant to an authorized investigation, as required by section 215).[11]

The second initiative—known as the *PRISM* or *section 702* program—involves the NSA's use of court orders issued under section 702 of FISA[12] to collect the content of certain international communications. The program involves the targeting of specific non-Americans

---

[5] *See, e.g.*, William C. Banks, *Programmatic Surveillance and FISA: Of Needles in Haystacks*, 88 TEX. L. REV. 1633 (2010).

[6] 50 U.S.C. § 1861.

[7] Glenn Greenwald, *NSA Collecting Phone Records of Millions of Verizon Customers Daily*, GUARDIAN (U.K.), June 5, 2013.

[8] Robert S. Litt, General Counsel, Office of the Director of National Intelligence, Newseum Special Program – NSA Surveillance Leaks: Fact and Fiction 8 (June 26, 2013) (transcript available at http://www.dni.gov/index.php/newsroom/speeches-and-interviews/195-speeches-interviews-2013/887-transcript-newseum-special-program-nsa-surveillance-leaks-facts-and-fiction?tmpl=component&format=pdf).

[9] *Id.*

[10] 442 US 735 (1979).

[11] *Available at* http://www.uscourts.gov/uscourts/courts/fisc/br13-09-primary-order.pdf [hereinafter Section 215 Ruling]; *see also* Charlie Savage, *Extended Ruling by Secret Court Backs Collection of Phone Data*, N.Y. TIMES, Sept. 17, 2013.

[12] 50 U.S.C. § 1881a.

who are reasonably believed to be located outside the country, as well as bulk collection of some foreign-to-foreign communications that happen to be passing through telecommunications infrastructure in the United States.[13] The FISA court does not approve individual surveillance applications each time the NSA wishes to intercept these communications; instead, it issues once-a-year blanket authorizations.[14] As detailed below, in 2011 the FISA court struck down the program on constitutional and statutory grounds after the government disclosed that it was inadvertently intercepting a significant number of communications involving Americans;[15] the court upheld the program shortly thereafter when the NSA devised a technical solution that prevented such overcollection.[16]

Programmatic surveillance initiatives like these differ in simple yet fundamental ways from the traditional forms of monitoring with which many people are familiar—monitoring that we might describe as *individualized* or *particularized* surveillance. Individualized surveillance takes place when authorities have some reason to think that a specific, known person is breaking the law. Investigators will then obtain a court order authorizing them to collect information about the target, with the goal of assembling evidence that can be used to establish his guilt in subsequent criminal proceedings. Individualized surveillance is common in the world of law enforcement, as under Title III of the Omnibus Crime Control and Safe Streets Act of 1968.[17] It is also used in national security investigations. FISA allows authorities to obtain a court order to engage in wiretapping if they demonstrate, among other things, probable cause to believe that the target is "a foreign power or an agent of a foreign power."[18]

By contrast, programmatic surveillance has very different objectives and is conducted in a very different manner. It usually involves the government collecting bulk data and then examining it to identify previously unknown terrorists, spies, and other national security threats. A good example of the practice is *link analysis*, in which authorities compile large amounts of information, use it to map the social networks of known terrorists—has anyone else used the same credit card as Mohamed Atta?—and thus identify associates with whom they may be conspiring.[19] (It's also possible, at least in theory, to subject these large databases to *pattern analysis*, in which automated systems search for patterns of behavior that are thought to be indicative of terrorist activity, but it's not clear that the NSA is doing so here.) Suspects who have been so identified can then be subjected to further forms of monitoring to determine their intentions and capabilities, such as wiretaps under FISA or other authorities. In a sense, programmatic surveillance is the mirror image of individualized surveillance. With



[13] Barton Gellman & Laura Poitras, *U.S., British Intelligence Mining Data from Nine U.S. Internet Companies in Broad Secret Program*, WASH. POST, June 6, 2013; Jonathan Hall, *Washington Post Updates, Hedges On Initial PRISM Report*, FORBES, June 7, 2013.

[14] 50 U.S.C. § 1881a(a).

[15] *Available at* http://www.lawfareblog.com/wp-content/uploads/2013/08/162016974-FISA-court-opinion-with-exemptions.pdf [hereinafter October 3, 2011 Section 702 Ruling].

[16] *See infra* notes 77-79 and accompanying text.

[17] 18 U.S.C. § 2518.

[18] 50 U.S.C. § 1805(a)(2)(A).

[19] MARK M. LOWENTHAL, INTELLIGENCE: FROM SECRETS TO POLICY 255 (4th ed. 2009).

individualized monitoring, authorities begin by identifying a suspect and go on to collect information; with programmatic monitoring, authorities begin by collecting information and go on to identify a suspect.

Programmatic surveillance has the potential to be a powerful counterterrorism tool. The Ra'ed al-Banna incident is a useful illustration of how the technique, when coupled with old-fashioned police work, can identify possible threats who otherwise might escape detection. Another example comes from a 2002 Markle Foundation study. According to that analysis, it would have been possible for authorities to identify all 19 of the 9/11 hijackers if they had assembled a large database of airline reservation information and subjected it to link analysis.[20] In particular, two of the terrorists—Nawaf al-Hamzi and Khalid al-Mihdhar—appeared on a government watchlist because they were known to have attended a January 2000 al Qaeda summit in Malaysia. So they could have been flagged when they bought their tickets. Querying the database to see if any other passengers had used the pair's mailing addresses would have led investigators to three more hijackers, including Mohamed Atta, the plot's operational leader. Six others could have been found by searching for passengers who used the same frequent-flyer and telephone numbers as these suspects. And so on. Again, the Markle study concerns passenger reservation data, not the communications data that are the NSA's focus. But it is still a useful illustration of the technique's potential.

The government claims that programmatic surveillance has been responsible for concrete and actual counterterrorism benefits, not just hypothetical ones. Officials report that the PRISM program in particular has helped disrupt about 50 terrorist plots worldwide, including ten in the United States.[21] Those numbers include Najibullah Zazi, who attempted to bomb New York City's subway system in 2009, and Khalid Ouazzani, who plotted to blow up the New York Stock Exchange. Authorities further report that PRISM played an important role in tracking down David Headley, an American who aided the 2008 terrorist atrocities in Bombay, and who in 2009 planned to attack the offices of a Danish newspaper that printed cartoons of Mohamed. The government also claims at least one success from the telephony metadata program, though it has been coy about the specifics: "The NSA, using the business record FISA, tipped [the FBI] off that [an] individual had indirect contacts with a known terrorist overseas. . . . We were able to reopen this investigation, identify additional individuals through a legal process and were able to disrupt this terrorist activity."[22] These claims have to be taken with a few grains of salt. Some commentators allege that the government could have thwarted these attacks using standard investigative techniques, and without resorting to extraordinary methods like programmatic surveillance.[23] And we should always be cautious when evaluating the merits of classified intelligence initiatives on the basis of selective and piecemeal revelations, as officials might tailor the information they release in a bid to shape public opinion.[24] But if specific claimed

[20] PROTECTING AMERICA'S FREEDOM IN THE INFORMATION AGE: A REPORT OF THE MARKLE FOUNDATION TASK FORCE 28 (2002); *see also* Baker & Sales, *supra* note 1, at 281-82.

[21] Sean Sullivan, *NSA Head: Surveillance Helped Thwart More Than 50 Terror Plots*, WASH. POST, June 18, 2013.

[22] *Id.*

[23] Abby Ohlheiser, *The NSA's Best Defense of PRISM Didn't Even Last a Week*, ATLANTIC WIRE, June 11, 2013.

[24] JAMES BAMFORD, BODY OF SECRETS: ANATOMY OF THE ULTRA-SECRET NATIONAL SECURITY AGENCY: FROM THE COLD WAR THROUGH THE DAWN OF A NEW CENTURY 384 (2001).

success remain contested, it still seems safe to conclude that programmatic surveillance can be a helpful resource in the counterterrorism toolkit.

As these examples imply, effective programmatic surveillance often requires government access to huge troves of information—e.g., large databases of airline passenger reservations, compilations of metadata concerning telephonic and internet communications, and so on. This is why it typically will not be feasible to limit bulk collection to particular, known individuals who are already suspected of being terrorists or spies. Some officials have taken to defending the NSA programs by pointing out that, "[i]f you're looking for the needle in a haystack, you have to have the haystack."[25] That metaphor doesn't strike me as terribly helpful; rummaging around in a mound of hay is, after all, a paradigmatic image of futility. But the idea can be expressed in a more compelling way. Programmatic surveillance cannot be done in a particularized manner. The whole point of the technique is to identify unknown threats to the national security; by definition, it cannot be restricted to threats that have already been identified. We can't limit programmatic surveillance to the next Mohamed Atta when we have no idea who the next Mohamed Atta is—and when, indeed, the goal of the exercise is precisely to identify the next Mohamed Atta.

Programmatic surveillance thus can help remedy some of the difficulties that arise when monitoring covert adversaries like international terrorists. FISA and other particularized surveillance tools are useful when authorities want to monitor targets whose identities are already known. But they are less useful when authorities are trying to identify unknown targets. The problem arises because, in order to obtain a wiretap order from the FISA court, the government usually must demonstrate probable cause to believe that the target is a foreign power or agent of a foreign power.[26] This is a fairly straightforward task when the target's identity is already known—e.g., a diplomat at the Soviet embassy in Washington, DC. But the task borders on the impossible when the government's reason for surveillance is to detect targets who are presently unknown—e.g., al Qaeda members who operate in the shadows. How can you convince the FISA court that Smith is an agent of a foreign power when you know nothing about Smith—his name, nationality, date of birth, location, or even whether he is one person or several dozen? The government typically won't know those things unless it has collected some information about Smith—i.e., unless it has surveilled him. Programmatic monitoring helps avoid the crippling Catch-22 that can arise under particularized surveillance regimes like FISA: Officials can't surveil unless they show that the target is a spy or terrorist, but they can't show that an unknown target is a spy or terrorist unless they have surveilled him.

## II.

While programmatic surveillance can be an important counterterrorism tool, it also—given the sweeping scope of the data collection on which it usually relies—raises profound concerns about civil liberties and privacy. These concerns are not merely hypothetical. To take just a few notorious examples of abusive monitoring, albeit of the particularized rather than

[25] Dana Bash & Tom Cohen, OFFICIALS CITE THWARTED PLOTS, OVERSIGHT IN DEFENDING SURVEILLANCE, CNN, June 19, 2013, http://www.cnn.com/2013/06/18/politics/nsa-leaks/index.html.

[26] 80 U.S.C. § 1805(a)(2)(A).

programmatic variety, the FBI repeatedly wiretapped Dr. Martin Luther King and his associates, purportedly to discover whether the civil rights leader had any ties to the Soviet Union.[27] And during the 1964 presidential campaign, LBJ aide Bill Moyers—yes, *that* Bill Moyers—directed the FBI to dig for evidence that some of Barry Goldwater's staffers were homosexuals.[28] The possibility of abuse makes it critical to establish a set of first principles to govern when and how programmatic monitoring is to be conducted. It is especially important to think about these baseline rules now, when the technique is still in its relative youth. This will allow programmatic surveillance to be nudged in privacy-protective directions as it develops into maturity. The critical question is how to take advantage of its potentially significant national security benefits without running afoul of fundamental civil liberties and privacy values. In other words, what can be done to domesticate programmatic surveillance?

This is not the place to flesh out the precise details of the ideal surveillance regime, but we can identify certain basic principles that academics, policymakers, and others should consider when thinking about bulk data collection and analysis. Two broad categories of principles should govern any such system; one concerns its formation, the other its implementation. First, there are the *architectural* or *structural* considerations—the principles that address when programmatic surveillance should take place, the process by which such a regime should be adopted, and how the system should be organized. Second, there are the *operational* considerations—the principles that inform the manner in which programmatic surveillance should be carried out in practice.

A.

As for the structural considerations, one of the most important is what might be called an *anti-unilateralism* principle. A system of programmatic surveillance should not be put into effect on the say-so of the executive branch, but rather should be a collaborative effort that involves Congress (in the form of authorizing legislation) and the judiciary (in the form of FISA court review of the initiatives).[29] An example of the former is FISA itself, which Congress enacted with the executive's reluctant consent in 1978. At the time, the NSA was engaged in fairly widespread bulk collection, without prior judicial approval, of certain international communications into and out of the United States—namely, by tapping into offshore telecommunications cables and by eavesdropping on satellite based radio signals. FISA's famously convoluted definition of "electronic surveillance"[30] can be seen as a congressional effort to preserve these preexisting practices, even as Congress was imposing a new requirement of judicial approval before conducting other kinds of surveillance.[31] An example of the latter concerns the warrantless Terrorist Surveillance Program, under which the NSA was intercepting, outside the FISA framework, certain communications between suspected al Qaeda figures

[27] David J. Garrow, *The FBI and Martin Luther King*, ATLANTIC, July/Aug. 2002, at 80.

[28] Laurence H. Silberman, *Hoover's Institution*, WALL ST. J., July 20, 2005.

[29] *See generally* JACK GOLDSMITH, THE TERROR PRESIDENCY 123-26, 205-07 (2007).

[30] 50 U.S.C. § 1801(f).

[31] David S. Kris, *Modernizing the Foreign Intelligence Surveillance Act*, *in* LEGISLATING THE WAR ON TERROR: AN AGENDA FOR REFORM 217, 224-25 (Benjamin Wittes ed., 2009).

overseas and people who were located in the United States. After that program's existence was revealed in late 2005, the executive branch persuaded the FISA court to issue orders allowing it to proceed subject to various limits.[32] (That accommodation eventually proved unworkable, and the executive then worked with Congress to put the program on a more solid legislative footing through the temporary Protect America Act of 2007[33] and the permanent FISA Amendments Act of 2008.[34])

Anti-unilateralism is important for several reasons. To take the most obvious, Congress and the courts can serve as external checks on executive overreach,[35] such as engaging in monitoring when it is not justified or using surveillance against political enemies or dissident groups. The risk of abuse is lessened if the executive branch must enlist its partners before commencing a new surveillance initiative. Congress might decline to permit bulk collection in circumstances where it concludes that ordinary, individualized monitoring would suffice, or it might authorize programmatic surveillance subject to various privacy protections. In addition, inviting many voices to the decisionmaking table increases the probability of sound outcomes. More participants with diverse perspectives can also help mitigate the groupthink tendencies to which the executive branch is sometimes subject.[36] If we're going to engage in programmatic surveillance, it should be the result of give and take among all three branches of the federal government, or at least between its two political branches, not the result of executive edict.

A second structural principle follows from the first: Programmatic surveillance should, where possible, have *explicit statutory authorization*. Congress does not "hide elephants in mouseholes,"[37] the saying goes, and we should not presume that Congress meant to conceal its approval of a potentially controversial programmatic surveillance system in the penumbrae and interstices of obscure federal statutes. Instead, Congress normally should use express and specific legislation when it wants to okay bulk data collection. Clear laws will help remove any doubt about the authorized scope of the approved surveillance, thereby promoting legal certainty. Express congressional backing also helps give the monitoring an air of legitimacy. And a requirement that programmatic surveillance usually should be approved by clear legislation helps promote accountability by minimizing the risk of congressional shirking.[38] If the political winds shift, and a legislatively approved program becomes unpopular, Congress will not be able to hide behind an ambiguous statutory grant of power and deflect responsibility to the President.

---

[32] David Kris, *A Guide to the New FISA Bill, Part II*, Balkinization (July 29, 2013, 12:45 PM), http://balkin.blogspot.com/2008/06/guide-to-new-fisa-bill-part-ii.html.

[33] Pub. L. No. 110-55, 121 Stat. 552 (2007).

[34] Pub. L. No. 110-261, 122 Stat. 2436 (2008).

[35] *See, e.g.*, JACK GOLDSMITH, POWER AND CONSTRAINT: THE ACCOUNTABLE PRESIDENCY AFTER 9/11, at xv (2012) ("[D]emocratic and judicial forces change presidential authorities and actions deemed imprudent or wrong and constrain presidential discretion in numerous ways."). *But see* ERIC A. POSNER & ADRIAN VERMEULE, THE EXECUTIVE UNBOUND: AFTER THE MADISONIAN REPUBLIC 4 (2010) (arguing that we now live in an "age after the separation of powers, and the legally constrained executive is now a historical curiosity").

[36] *See, e.g.*, Steve Smith, *Groupthink and the Hostage Rescue Mission*, 15 BRIT. J. POL. SCI. 117 (1984).

[37] Whitman v. Am. Trucking Ass'ns, 531 U.S. 457, 468 (2001).

[38] *See, e.g.*, Nicholas Quinn Rosenkranz, *Federal Rules of Statutory Interpretation*, 115 HARV. L. REV. 2085, 2155 (2002) (emphasizing that "ambiguity allows Congress to evade accountability").

Of course, exacting legislative clarity may not be possible in all cases. Sometimes, explicit statutory language might compromise intelligence sources and methods and thereby enable surveillance targets to evade detection,[39] or provoke a diplomatic row.[40] But clarity often will be feasible, and the Protect America Act and FISA Amendments Act are good examples of what the process could look like. In both cases, Congress clearly and unambiguously approved monitoring that the executive branch previously claimed[41] was implicitly authorized by a combination of FISA (which at the time made it unlawful to engage in electronic surveillance "except as authorized by statute"[42]), the September 18, 2001 Authorization for Use of Military Force (which authorizes the president to use "all necessary and appropriate force" against those responsible for the 9/11 terrorist attacks[43]), and the Supreme Court's decision in *Hamdi v. Rumsfeld* (which interpreted the AUMF's reference to "all necessary and appropriate force" to include "fundamental and accepted" incidents of war, such as detention[44]).

Next, there is the question of *transparency*. Whenever possible, programmatic surveillance systems should be adopted through open and transparent debates that allow an informed public to meaningfully participate. The systems also should be operated in as transparent a manner as possible. This in turn requires the government to reveal enough information about the proposed surveillance, even if at a fairly high level of generality, that the public is able to effectively weigh its benefits and costs. Transparency is important because it helps promote accountability; it enables the public to hold their representatives in Congress and the executive branch responsible for the choices they make. "[I]nformed public opinion is the most potent of all restraints upon misgovernment."[45] Transparency also fosters democratic participation, ensuring that the people are ultimately responsible for deciding what our national security policies should be. And it can help dispel suspicions about programs that initially might seem nefarious but end up looking innocuous when their details are known.[46] Again, perfect transparency will not always be feasible—a public debate about the fine-grained details of proposed surveillance can compromise extremely sensitive intelligence sources and methods. But transparency should be the default rule, and even where the government's operational needs rule out detailed disclosures, a generic description of a proposed program is better than none at all.

---

[39] *See, e.g.*, CIA v. Sims, 471 U.S. 159, 167 (1985).

[40] *See, e.g.*, Peter P. Swire, *The System of Foreign Intelligence Surveillance Law*, 72 GEO. WASH. L. REV. 1306, 1323 (2004).

[41] Letter from William E. Moschella, Assistant Att'y Gen., Off. of Legis. Aff., U.S. Dep't of Justice., to Pat Roberts, Chairman, Senate Select Comm. on Intelligence, et al. (Dec. 22, 2005), *available at* http://www.fas.org/irp/agency/doj/fisa/doj122205.pdf.

[42] 50 U.S.C. § 1809(a)(1) (2000).

[43] Pub. L. No. 107-40, § 2(a), 115 Stat. 224 (2001).

[44] 542 U.S. 507, 518 (2004).

[45] Grossjean v. Am. Press Co., 297 U.S. 233, 250 (1936).

[46] *See, e.g.*, Richard Gid Powers, *Introduction* to DANIEL PATRICK MOYNIHAN, SECRECY: THE AMERICAN EXPERIENCE 58 (1998) (emphasizing that a lack of transparency "gives rise to fantasies that corrode belief in the possibilities of democratic government").

Finally, any programmatic surveillance regime should observe an *anti-mission-creep* principle. Bulk data collection should only be used to investigate and prevent terrorism, espionage, and other serious threats to the national security. It should be off limits in regular criminal investigations. Moreover, if programmatic surveillance happens to turn up evidence of ordinary crime, intelligence officials normally should not be able to refer it to their law enforcement counterparts for prosecution—though there should be an exception for truly grave crimes, such as offenses involving a risk of death or serious bodily injury and crimes involving the exploitation of children. This is a simple matter of costs and benefits. The upside of preventing deadly terrorist attacks and other national security perils can be so significant that we as a nation may be willing to sanction extraordinary investigative techniques like bulk data collection. But the calculus looks very different where the promised upside is prosecuting garden-variety crimes like income tax evasion or insurance fraud. We might be willing to tolerate an additional burden on our privacy interests to stop the next 9/11, but that doesn't mean we should make the same sacrifice to stop tax cheats and fraudsters.

B.

As for the operational considerations, among the most important is the need for *external checks* on programmatic surveillance, whether judicial, legislative, or both. In particular, bulk data collection should have to undergo some form of judicial review, such as by the FISA court, in which the government demonstrates that it meets the applicable constitutional and statutory standards. Ideally, the judiciary would give its approval before collection begins. But this will not always be possible, in which case timely post-collection judicial review will have to suffice. (FISA has a comparable mechanism for temporary warrantless surveillance in emergency situations.[47]) Programmatic surveillance also should be subject to robust congressional oversight. This could take a variety of forms, including informal consultations with members of Congress when designing the surveillance regime (including, at a minimum, congressional leadership and members of the applicable committees), as well as regular briefings to appropriate personnel on the operation of the system and periodic oversight hearings.

Oversight by the courts and Congress provides an obvious, first-order level of protection for privacy and civil liberties—an external veto serves as a direct check on possible executive misconduct. Judicial and legislative checks also offer a less noticed but equally important second-order form of protection. The mere possibility of an outsider's veto can have a chilling effect on executive misconduct, discouraging officials from questionable activities that would have to undergo, and might not survive, external review.[48] Moreover, external checks can channel the executive's scarce resources into truly important surveillance and away from relatively unimportant monitoring. This is so because oversight increases the costs of collecting bulk data—e.g., preparing a surveillance application, persuading the judiciary to approve it, briefing the courts and Congress about how the program has been implemented, and so on. These increased costs encourage the executive to prioritize collection that is expected to yield

[47] 50 U.S.C. § 1805(e).

[48] *See, e.g.*, Nathan Alexander Sales, *Self-Restraint and National Security*, 6 J. NAT'L SEC. L. & POL'Y 227, 280 (2012).

truly valuable intelligence and, conversely, to forego collection that is expected to produce information of lesser value.

Of course, judicial review in the context of bulk collection won't necessarily look the same as it does in the familiar setting of individualized monitoring of specific targets. If investigators want to examine a particular terrorism suspect's telephony metadata, they apply to the FISA court for a pen register / trap and trace order upon a showing that the information sought is relevant to an ongoing national security investigation.[49] But, as explained above, that kind of particularized showing usually won't be possible where authorities are dealing with unknown threats, and where the very purpose of the surveillance is to identify the threats. In these situations, reviewing courts may find it necessary to allow the government to collect large amounts of data without an individualized showing of relevance. This doesn't mean that privacy safeguards must be abandoned and the executive given free rein. Instead, courts could require that authorities demonstrate some level of individualized suspicion before they access the data that has been collected. Protections for privacy and civil liberties can migrate from the front end of the intelligence cycle to later stages.[50]

In more general terms, because programmatic surveillance involves the collection of large troves of data, it likely means some dilution of the familiar ex ante restrictions that protect privacy by constraining the government from acquiring information in the first place. It therefore becomes critically important to devise meaningful ex post safeguards that can achieve similar forms of privacy protection. In short, meaningful restrictions on the government's ability to access and use data that it has gathered must substitute for restrictions on the government's ability to gather that data at all; what I have elsewhere called *use limits* must stand in for *collection limits*.[51]

In addition to oversight by outsiders, a programmatic surveillance regime also should feature a system of *internal checks* within the executive branch, to review collection before it occurs, after the fact, or both. As for the ex ante checks, internal watchdogs should be charged with scrutinizing proposed bulk collection to verify that it complies with the applicable constitutional and statutory rules, and also to ensure that appropriate protections are in place for privacy and civil liberties. The Justice Department's Office of Intelligence is a well known example. The unit, which presents the government's surveillance applications to the FISA court, subjects proposals to exacting scrutiny, sometimes including multiple rounds of revisions, with the goal of increasing the likelihood of surviving judicial review.[52] Indeed, the office has a strong incentive to ensure that the applications it presents are in good order, so as to preserve its credibility with the FISA court.[53] Ex post checks include such commonplace mechanisms as

[49] 50 U.S.C. § 1842.

[50] *See* LOWENTHAL, *supra* note 19, at 55-67 (describing various stages of the intelligence cycle, including collection, processing and exploitation, analysis, and dissemination).

[51] Nathan Alexander Sales, *Run for the Border: Laptop Searches and the Fourth Amendment*, 43 U. RICH. L. REV. 1091, 1124-27 (2009).

[52] Sales, *Self-Restraint*, supra note 48, at 259-60.

[53] *Id*. at 285-86.

agency-level inspectors general, who can audit bulk collection programs, assess their legality, and make policy recommendations to improve their operation, as well as entities like the Privacy and Civil Liberties Oversight Board, which perform similar functions across the executive branch as a whole. Another important ex post check is to offer meaningful whistleblower protections to officials who know about programs that violate constitutional or statutory requirements. Allowing officials to bring their concerns to ombudsmen within the executive branch can help root out lawlessness and also relieve the felt necessity of leaking information about highly classified programs to the media.

These and other mechanisms can be an effective way of preventing executive misconduct. Done properly, internal checks can achieve all three of the benefits promised by traditional judicial and legislative oversight—executive branch watchdogs can veto surveillance they conclude would be unlawful, the mere possibility of such vetoes can chill overreach, and increasing the costs of monitoring can redirect scarce resources toward truly important surveillance. External and internal checks thus operate together as a system; the two types of restraints are rough substitutes for one another. If outside players like Congress and the courts are subjecting the executive's programmatic surveillance activities to especially rigorous scrutiny, the need for comparably robust safeguards within the executive branch tends to diminish. Conversely, if the executive's discretion is constrained internally through strict approval processes, audit requirements, and so on, the legislature and judiciary may choose not to hold the executive to the exacting standards they otherwise would. In short, certain situations may see less need to use traditional interbranch separation of powers and checks and balances to protect privacy and civil liberties, because the executive branch is subject to an "internal separation of powers"[54] that can accomplish much the same thing.

A word of caution. It's important not to take in-house review too far. Internal oversight can do more than deter overreach. It can also deter necessary national security operations, with potentially deadly results. The pre-9/11 information sharing wall is a notorious example of an internal check gone awry. The predecessor of DOJ's Office of Intelligence interpreted FISA to sharply restrict intelligence officials from coordinating or sharing information with their law enforcement counterparts, leading one prophetic FBI agent to lament on the eve of 9/11 that "someday somebody will die."[55] Indeed, DOJ was so committed to the wall that one senior official successfully lobbied the chief judge of the FISA court to issue an order formally imposing the wall requirements, which up to then had only taken the form of internal Justice Department guidelines.[56] There are other examples as well. In the 1990s, executive branch lawyers vetoed CIA plans to use targeted killing against Osama bin Laden, and members of the armed forces' Judge Advocate General corps have occasionally ruled out strikes on policy grounds even though they would be permissible under the laws of war.[57] There is no universally

[54] Neal Kumar Katyal, *Internal Separation of Powers: Checking Today's Most Dangerous Branch from Within*, 115 YALE L.J. 2314 (2006).

[55] NATIONAL COMMISSION ON TERRORIST ATTACKS UPON THE UNITED STATES, THE 9/11 COMMISSION REPORT 271 (2004).

[56] STEWART A. BAKER, SKATING ON STILTS: WHY WE AREN'T STOPPING TOMORROW'S TERRORISM TODAY 57 (2010).

[57] Sales, *Self-Restraint*, supra note 48, at 247-56.

applicable answer to the question, *how much internal oversight is enough?* Too little imperils privacy, too much threatens security. The right balance cannot be known a priori, but rather must be struck on a case by case basis taking account of the highly contingent and unique circumstances presented by a given surveillance program, the threat it seeks to combat, the privacy concerns it raises, and other factors.

A third operational consideration is the need for strong *minimization requirements*. Virtually all surveillance raises the risk that officials will intercept innocuous data in the course of gathering evidence of illicit activity. Inevitably, some chaff will be swept up with the wheat. The risk is especially acute with programmatic surveillance, in which the government assembles large amounts of data in the search for clues about a small handful of terrorists, spies, and other national security threats.[58] Minimization is one way to deal with the problem. Minimization rules limit what the government may do with data that does not appear pertinent to a national security investigation—e.g., how long it may be retained, the conditions under which it will be stored, the rules for accessing it, the purposes for which it may be used, the entities with which it may be shared, and so on. Congress appropriately has required intelligence officials to adopt minimization procedures, both under FISA's longstanding particularized surveillance regime[59] and under the more recent authorities permitting bulk collection.[60] But the rules need not be identical. Because programmatic surveillance often involves the acquisition of a much larger trove of non-pertinent information, the minimization rules for bulk collection ideally would contain stricter limits on the use of information unrelated to national security threats. In other words, the minimization procedures should reflect the *anti-mission-creep* principle described above and limit the use of inadvertently collected information for purposes unrelated to national security.

Finally, programmatic surveillance systems should have *technological safeguards* that protect privacy and civil liberties by restricting access to sensitive information and tracking what officials do with it.[61] As Larry Lessig has emphasized, software features that make it impossible to engage in certain undesirable conduct can substitute for legal prohibitions on the same behavior; code is law.[62] In particular, permissioning and authentication technologies can help ensure that sensitive databases are only available to officials who need them to perform various counterterrorism functions. And auditing tools can track who accesses the information, when, in what manner, and for what purposes. These mechanisms show promise but have a mixed record at preventing unauthorized access to and use of sensitive data. Access logs helped the State Department quickly identify and discipline the outside contractors who improperly accessed the private passport files of various presidential candidates in 2008.[63] But government employees like Edward Snowden and Bradley Manning obviously have been able to exfiltrate huge amounts of classified information from protected systems, either because technological controls were not

[58] LOWENTHAL, *supra* note 19, at 72-73.

[59] 50 U.S.C. §§ 1801(h), 1805(a)(3).

[60] *Id*. § 1881a(c)(1)(A), (e).

[61] *See, e.g.*, BAKER, *supra* note 56, at 334-41; MARKLE FOUNDATION, *supra* note 17, at 15, 17, 19, 33.

[62] LAWRENCE LESSIG, CODE VERSION 2.0, at 5-6 (2006).

[63] Glenn Kessler, *Rice Apologizes For Breach of Passport Data*, WASH. POST., Mar. 22, 2008.

in place or because they were able to evade them. Even if these mechanisms are not now an infallible safeguard against abuse, the basic principle seems sound: A commitment to privacy can be baked into a programmatic surveillance regime at the level of systems architecture.

III.

Judged by these standards, how well do the NSA initiatives measure up? As far as we can tell from the incomplete publicly available information, they fare well along several dimensions. But in other respects the programs should be adjusted to better conform to the first principles sketched out above. Several relatively modest reforms would preserve the essential features of the programs but ensure more robust protections for privacy and civil liberties.

Before turning to areas that need improvement, it's worth spending a few moments considering what the government has gotten right. One of the most noteworthy features of the NSA programs is their rejection of unilateralism. Rather than justifying the collection of international communications and telephony metadata on the basis of its own constitutional authorities, the executive branch in both instances has sought to ground its conduct in statutory powers conferred on it by Congress. This anti-unilateralism is especially significant because it is something of an historical anomaly; the executive routinely has undertaken national security surveillance without legislative backing. Consider, for example, wiretaps in the pre-FISA era, which were grounded solely in the president's constitutional powers,[64] or the executive's unilateral conduct of physical searches before FISA was amended in the 1990s to expressly authorize that activity,[65] or the warrantless Terrorist Surveillance Program of the early 2000s.

Of course, Congress has been much more explicit about approving the section 702 program—which, after all, takes its name from the section of FISA that specifically and expressly authorizes it—than the telephony metadata initiative. The latter is said to be based on FISA's business records authority, enacted in section 215 of the USA PATRIOT Act, which allows officials to obtain a FISA court order requiring the production of "any tangible things" upon a showing that they are "relevant."[66] Section 215 is often understood as a national security counterpart to the rules governing grand jury subpoenas. Yet the government is using it to collect a great deal more information than a typical subpoena obtains, and at least one legislator who was actively involved in crafting the statute claims that Congress never intended it to be used in this way.[67] To put it mildly, section 215 is a more roundabout authorization than section 702.

Yet Congress has been involved in approving the metadata program, albeit less explicitly and transparently than is ideal. Section 215 is a temporary statutory that is subject to periodic renewals. During the congressional debates over reauthorization in 2010 and 2011, the

[64] *See* Swire, *supra* note 40, at 1313-14.

[65] *See* William C. Banks & M.E. Bowman, *Executive Authority for National Security Surveillance*, 50 AM. U. L. REV. 1, 77 (2000).

[66] 50 U.S.C. § 1861(a)(1), (b)(2)(A).

[67] *See* Letter from Rep. F. James Sensenbrenner, Jr. to Attorney General Eric H. Holder, Jr., Jun. 6, 2013, *available at* http://sensenbrenner.house.gov/uploadedfiles/sensenbrenner_letter_to_attorney_general_eric_holder.pdf.

intelligence community prepared classified briefing materials that laid out unusually vivid details about the program.[68] The briefing papers described what information is collected, when the database may be queried, and—critically—the fact that the program is operated "pursuant to the 'business records' provision of the Foreign Intelligence Surveillance Act (FISA) (commonly referred to as 'section 215')." Officials further asked that the materials be shared with "all Members of Congress." In 2010 and again the following year, the Chairman and Vice Chairman of the Senate Select Committee on Intelligence circulated "Dear Colleague" letters encouraging senators to review the briefing.[69] On the House side, in 2010 a member of the Permanent Select Committee on Intelligence made a floor statement urging colleagues to review the materials.[70] (He does not appear to have renewed the invitation in 2011.) In addition to making these written materials available, administration officials reportedly conducted 13 in-person classified briefings for members about the section 215 program.[71]

Members of Congress who learned from these briefings that the executive branch was interpreting section 215 to authorize the telephony metadata program, and who then voted to reauthorize that legislation, can be said at some level to have embraced the executive's interpretation. Congress in 2001 may not have understood section 215 as anything more than a routine subpoena-like tool for the national security context. But Congress in 2010 and 2011 was put on notice that the executive branch was now reading the statute more expansively to authorize bulk data collection. In any event, the critical point is not, as the FISA court and some commentators have concluded,[72] that Congress's reauthorization votes effectively ratified the executive's interpretation of section 215. What matters for our purposes is that the executive went to unusual lengths to involve inform Congress about the program in an effort to obtain its assent.

In addition to Congress, the FISA court plays a key role in overseeing the NSA programs. Both initiatives involve various forms of ex ante judicial scrutiny. The telephony metadata program is reviewed every three months, when a prior court order authorizing collection expires and comes up for renewal. The court most recently reauthorized the program on July 19, 2013,[73] and it issued an opinion on August 29 detailing its conclusion that the program is constitutionally and statutorily permissible.[74] Likewise, the FISA court examines the government's section 702 surveillance applications before approving collection of certain international communications for

---

[68] *Available at* http://www.dni.gov/files/documents/2009_CoverLetter_Report_Collection.pdf, http://www.dni.gov/files/documents/2011_CoverLetters_Report_Collection.pdf.

[69] http://big.assets.huffingtonpost.com/SelectCommitteeIntelligenceFeb13.pdf.

[70] 156 Cong. Rec. H838 (daily ed. Feb. 25, 2010) (statement of Rep. Hastings).

[71] Josh Gerstein, *Official: 13 Briefings for Hill on Call-Tracking Legal Provision*, POLITICO, June 8, 2013.

[72] Section 215 Ruling, *supra* note 11, at 23-27; Posting of Benjamin Wittes & Jane Chong to Lawfare, http://www.lawfareblog.com/2013/09/congress-is-still-naked/ (Sept. 19, 2013, 12:03 AM). *But see* Posting of Orin Kerr to The Volokh Conspiracy, http://www.volokh.com/2013/09/17/thoughts-august-2013-fisc-opinion-section-215/ (Sept. 17, 2013, 7:39 PM) (criticizing FISA court's ratification analysis).

[73] Joby Warrick, *NSA Surveillance Program Extended by Court, Intelligence Officials Say*, WASH. POST, July 19, 2013.

[74] Savage, *supra* note 11.

a period of one year.[75] The court is also responsible for reviewing and approving the minimization procedures that govern how both programs operate in practice.[76] Again, the FISA court's role in overseeing programmatic surveillance represents a sharp departure from the historic norm. In the 1980s, when the NSA was engaging in bulk collection of satellite-based international communications (which Congress specially exempted from regulation under FISA), the court played no part in overseeing those operations.

The FISA court is often derided as a rubber stamp for the government's surveillance requests. But recently declassified documents suggest that the FISA court can in fact be a meaningful check on the executive branch.[77] In May 2011, the administration told the FISA court about an overcollection problem in the PRISM program. Because of the way some communications are bundled, the NSA had been collecting purely domestic communications in the course of intercepting communications involving persons reasonably believed to be outside the United States. After a series of written submissions, meetings between court and government personnel, and a hearing, the court on October 3, 2011 issued an 81-page opinion concluding that the program violated both the Fourth Amendment and FISA section 702, principally because the NSA's minimization procedures were inadequate.[78] The government responded by developing new procedures to segregate the permissible intercepts from the impermissible ones, applying the procedures to previous acquisitions, and purging tainted records from its database. The FISA court then ruled in opinions dated November 30, 2011 and September 25, 2012 that the revised program passed muster.

At one level this is a dismayingly familiar story of government misconduct. But the deeper lesson the episode reveals is that, when confronted with such misconduct, the FISA court is willing to intervene and enforce basic constitutional and statutory guarantees—which is exactly what we would expect an Article III court to do. The PRISM incident also suggests that the government takes seriously its obligations to self-police and disclose problems to the court. Indeed, officials have an interest in doing so. The government's ability to persuade the FISA court to approve its surveillance requests depends in large part on its credibility with the judges. And that goodwill would take a severe hit if the court independently learned, such as though leaks, about violations that officials had failed to disclose. It would be a mistake to take too much comfort from this incident, since it's impossible to say how representative it is. (Though a 2009 episode involving the telephony metadata program followed a similar pattern—discovery of violations through self-policing, disclosure to the FISA court, judicial rebuke, institution of reforms, and judicial approval of the revised program.[79]) Still, it provides some reason for optimism that FISA court oversight—and the internal oversight on which it depends—is more than perfunctory.



---

[75] 50 U.S.C. § 1881a(a).

[76] *Id*. §§ 1861(g) (section 215 program), 1881a(e) (section 702 program).

[77] *See* Ellen Nakashima, *NSA Gathered Thousands of Americans' E-mails Before Court Ordered It to Revise Its Tactics*, WASH. POST, Aug. 21, 2013.

[78] October 3, 2011 Section 702 Ruling, *supra* note 15.

[79] Ellen Nakashima et al., *Declassified Court Documents Highlight NSA Violations in Data Collection for Surveillance*, WASH. POST, Sept. 10, 2013.

A third noteworthy feature of PRISM, though not the metadata program, is the unusual transparency surrounding its adoption. PRISM appears to be a straightforward application of FISA section 702, which Congress enacted in 2008. The legislation was the result of a lengthy and detailed public debate touched off by revelations in late 2005 that the Terrorist Surveillance Program was intercepting certain international communications without judicial approval. During the ensuing three year national conversation, intelligence officials repeatedly explained to Congress and the public why they thought new statutory authority was necessary, and advocacy groups and other interested parties repeatedly challenged these representations and urged Congress to reject, or at least curtail, any new surveillance powers. Newspaper editorial pages, blogs, talk radio programs, and many other media organs hashed out the legal and policy issues. FISA was front page news. In short, the section 702 program shouldn't come as a surprise because the nation thoroughly debated it for three years before Congress expressly approved it.

While the NSA programs reflect a number of important safeguards to help protect privacy and civil liberties, there is still room for improvement. Policymakers should consider altering the minimization rules to better prevent mission creep, adding an adversarial element to certain aspects of the FISA court's proceedings, and enacting new legislation to place the telephony metadata program on a more stable statutory footing.

First, the minimization rules that govern the section 702 program allow intelligence officials to share information with federal law enforcement if it contains "evidence of a crime."[80] This seems too permissive. On their face, the rules permit the fruits of PRISM surveillance to be used in investigations of even minor federal offenses, such as mail fraud and theft. The problem is that the relative costs and benefits of surveillance depend on the magnitude of the offense under investigation. Just because we're willing to countenance the use of extraordinary methods to prevent terrorism doesn't mean the same techniques should be used to combat tax delinquency. Policymakers should consider tightening the list of crimes for which sharing is allowed. Of course, intelligence officials certainly should be able to tell their law enforcement counterparts when they come across evidence of terrorism, espionage, and other national security threats—the need for cops and spies to share more counterterrorism information is one of the enduring lessons of 9/11.[81] And other serious crimes like those involving risk of death or serious bodily injury, or child exploitation, should be on the list as well.

At the same time, we shouldn't overestimate the NSA's enthusiasm for sharing the intelligence it gathers. Regardless of what the minimization rules permit, the NSA will have strong incentives to resist sharing information with or otherwise helping its bureaucratic rivals.[82] Indeed, the *New York Times* recently reported widespread frustration among law enforcement officials over the NSA's reluctance to assist their investigations of routine offenses like "money

[80] Minimization Procedures Used by the National Security Agency in Connection with Acquisitions of Foreign Intelligence Information Pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, as Amended (July 28, 2009), *available at* https://s3.amazonaws.com/s3.documentcloud.org/documents/716634/exhibit-b.pdf.

[81] *See, e.g.*, 9/11 COMMISSION REPORT, *supra* note 55, at 416-19.

[82] *See* Nathan Alexander Sales, *Share and Share Alike: Intelligence Agencies and Information Sharing*, 78 GEO. WASH. L. REV. 279 (2010).

laundering, counterfeiting and even copyright infringement"; their requests are usually denied "because the links to terrorism or foreign intelligence" are considered too "tenuous."[83] (Note that the story addresses NSA resources in general, not telephony metadata and PRISM data in particular.) In short, institutional self-interest and legal restrictions on sharing can be rough substitutes. And while self-interest will often lead the NSA to refuse access to sensitive intelligence in garden variety criminal cases, these naturally occurring bureaucratic incentives should be supplemented with strong minimization rules that prevent inappropriate mission creep.

Second, Congress's decision to subject the executive branch's surveillance requests to ex ante judicial review—one of the most important innovations of the original 1978 FISA—has created a powerful tool for preventing overreach. But this mechanism has its limits, because the FISA court's proceedings are conducted ex parte.[84] This can deprive the court of the benefits of the ordinary adversarial process, which relies on the presentation of opposing points of view to sharpen and refine legal and factual disputes. For that reason, policymakers should consider providing for adversarial review in the FISA court in certain circumstances. Indeed, there is some precedent for doing so. In 2002, when the FISA court of review sat for the first time in its history to consider the constitutionality of the USA PATRIOT Act's alteration of FISA's "primary purpose" standard, the appellate court invited outside groups that were critical of the changes to participate as *amici curiae*.[85]

This is not to suggest that the process for approving surveillance is entirely lacking in adversarialism. Adversarial review is present, it just takes place in the executive branch rather than the FISA court. Surveillance applications typically undergo multiple layers of internal review before presentation to the court, and that process can be exacting. The unit that manages the review process—the Justice Department's Office of Intelligence—routinely pushes back on operators seeking permission to engage in surveillance.[86] The office might insist that the application include more facts to support the claim that a target is a spy or terrorist. Or it might demand a fuller explanation of the expected national security gains. Or it might require stricter privacy rules governing how collected information is to be used. Again, self-interest explains why.[87] Office lawyers want to maintain their enviable record before the FISA court, so they closely scrutinize the proposals that land on their desk. If they seem unlikely to meet the court's approval, they are sent back for revision or rejected outright. This kind of internal review may not be a perfect substitute for a traditional adversarial hearing before a court, but it can achieve some of the same benefits.

Nor is this to suggest that *all* FISA court proceedings should contain an adversarial element. The bulk of the court's work is reviewing individualized applications to monitor specific targets, and the benefits of an adversarial process would be relatively slight in this

---

[83] Eric Lichtblau & Michael S. Schmidt, *Other Agencies Clamor for Data N.S.A. Compiles*, N.Y. TIMES, Aug. 3, 2013.

[84] 50 U.S.C. § 1805(a).

[85] *In re:* Sealed Case, 310 F.3d 717 (2002).

[86] *See, e.g.*, BAKER, *supra* note 56, at 54-55.

[87] Sales, *Self-Restraint*, supra note 48, at 285-86.

context. This is familiar ground for federal judges, who routinely approve individualized wiretaps ex parte in regular criminal investigations.[88] Moreover, cutting edge legal and policy issues are less likely to arise in the course of adjudicating a request to tap a specific person, as these proceedings usually turn on an essentially factual question—i.e., is there probable cause to believe the target is an agent of a foreign power? Adversarial proceedings would be more helpful in circumstances where the court is asked to approve broad, overarching surveillance programs like the metadata and PRISM initiatives. These sorts of proceedings frequently will involve the balancing of basic values like the need to preserve both national security and privacy and civil liberties. In that respect the proceedings can be quasi-legislative and thus would benefit from the presence of diverse viewpoints.

What could adversarial review look like in practice? It wouldn't be realistic to rely on outsiders, such as advocacy groups or telecommunications carriers, to oppose the government before the FISA court. Doing so would require access to a great deal of highly classified information about extremely sensitive surveillance programs, and the government will have strong reasons to resist giving outsiders the requisite security clearances. The better course would be to establish a sort of "devil's advocate" within the executive branch. The process could resemble the intelligence technique known as "red teaming," in which special groups of analysts improve intelligence products by preparing assessments that challenge the conventional wisdom.[89] Adversarial review could be the default rule, but there could be a mechanism to bypass the process in specified emergency situations. In those circumstances, the government would be able to initiate surveillance without an adversarial hearing, but would have to submit to normal adversarial review as soon as possible and would have to terminate the surveillance if the FISA court ultimately concludes that it is unjustified. (Again, FISA's mechanism for emergency wiretaps could serve as inspiration.[90])

Finally, officials should reconsider whether section 215 is the appropriate statutory vehicle for the telephony metadata program. It seems a stretch use the equivalent of a grand jury subpoena to collect billions of call records. Moreover, some have questioned whether the program comports with a strict reading of the statutory requirements.[91] Are electronic records (or databases of electronic records) "tangible things" within the meaning of section 215? Is an entire database deemed "relevant" because it contains a handful of records pertinent to counterterrorism efforts? The NSA may well have good reasons to assemble large databases of telephony metadata, but section 215 seems like an awkward way to do it. Congress should consider enacting new legislation that specifically authorizes the program in clear and express terms, and describes the limits under which it may operate. This is precisely what Congress did in the FISA Amendments Act of 2008, which placed the Terrorist Surveillance Program on solid statutory ground; Congress could follow a similar approach here.



[88] 18 U.S.C. § 2518(3).

[89] LOWENTHAL, *supra* note 19, at 135, 139.

[90] 50 U.S.C. § 1805(e).

[91] *See, e.g.*, Jaffer, *supra* note 4.

***

Big data is probably here to stay. Programmatic surveillance that aims at identifying previously unknown terrorists and spies has the potential to be an important addition to the national security toolkit. And in an era where private companies like Amazon and Google assemble detailed digital dossiers to predict their customers' buying habits, it's more or less inevitable that counterterrorism officials will want to take advantage of the same sorts of technologies to stop the next 9/11. That's why it's critical to establish a set of baseline rules to govern any system of programmatic surveillance. These first principles can ensure that the government is equipped a valuable tool for preventing terrorist atrocities while simultaneously preserving our national commitment to civil liberties and privacy.

Draft © 11/4/2013; Please Do Not Cite Without Permission
9 I/S: J.L. & POL'Y FOR INFO. SOC'Y (forthcoming 2014)

# STANDING AND SECRET SURVEILLANCE

**Stephen I. Vladeck**†

On February 26, 2013, a 5-4 majority of the U.S. Supreme Court held in *Clapper* v. *Amnesty International USA*[1] that a coalition of attorneys and human rights, labor, legal, and media organizations lacked Article III standing to pursue their constitutional challenge to section 702 of the Foreign Intelligence Surveillance Act (FISA).[2] Section 702—the central innovation of the FISA Amendments Act of 2008 (FAA)—provided new statutory authorization for mass electronic surveillance targeting communications of non-U.S. persons outside the United States. And although Congress expressly barred the use of section 702 to intentionally target communications by U.S. persons,[3] the plaintiffs in *Clapper* alleged that the surveillance authorized by section 702 made it far more likely that such communications would nevertheless be intercepted. Given that section 702 requires no showing of individualized suspicion before such communications are obtained,[4] the plaintiffs argued that it would therefore be unconstitutional.[5]

In rejecting the plaintiffs' standing to pursue such claims, Justice Alito's opinion for the *Clapper* Court seized upon the secret nature of the alleged governmental surveillance that the plaintiffs sought to challenge.[6]

---

† Professor of Law and Associate Dean for Scholarship, American University Washington College of Law. Thanks to Peter Shane for inviting me to participate in this symposium (and for helpful feedback on an earlier draft), and to Caitlin Marchand, American University Washington College of Law Class of 2015, and Mary Van Houten, Stanford Law School Class of 2014, for research assistance. In the interest of full disclosure, readers should know that I co-authored an amicus brief on behalf of the Petitioner in *In re EPIC*, No. 13-58 (U.S. filed Aug. 12, 2013). Needless to say, the views expressed herein are mine alone.

1. 133 S. Ct. 1138 (2013).

2. Pub. L. No. 95-511, 92 Stat. 1783 (1978) (codified at 50 U.S.C. §§ 1801 *et seq.*). Section 702 was added to FISA by the FISA Amendments Act of 2008 (FAA), Pub. L. No. 110-261, § 101, 122 Stat. 2436, 2438–48 (codified at 50 U.S.C. § 1881a).

3. *See* 50 U.S.C. § 1881a(b).

4. *See id.* §§ 1881a(a), (g).

5. *See* Amnesty Int'l USA v. Clapper, 638 F.3d 118, 121 (2d Cir. 2011), *rev'd*, 133 S. Ct. 1138.

6. *Clapper*, 133 S. Ct. at 1148 ("[R]espondents have no actual knowledge of the Government's § 1881a targeting practices. Instead, respondents merely speculate and make

Because such secrecy prevented the plaintiffs from showing that the government's interception of their communications was "certainly impending," they could not establish the injury-in-fact required by the Court's prior interpretations of Article III's case-or-controversy requirement.[7] Of course, the upshot of Justice Alito's analysis is obvious: given that the actual implementation of such surveillance authority is highly classified, it would be virtually impossible for any individual to *ever* satisfy the "certainly impending" standard that his majority opinion articulates. *Clapper* thereby appeared to insulate the government's secret surveillance programs—under section 702 or otherwise—from all external judicial challenge.[8]

In retrospect, the timing of the Supreme Court's decision in *Clapper* was rather ironic. Less than three months later, the *Washington Post* published details on the hitherto-secret "PRISM" program, pursuant to which the government, acting under section 702, has been "tapping directly into the central servers of nine leading U.S. Internet companies, extracting audio and video chats, photographs, e-mails, documents, and connection logs."[9] And another Snowden-based story from late October revealed that "[t]he National Security Agency has secretly broken into the main communications links that connect Yahoo and Google data centers around the world,"[10]

---

assumptions about whether their communications with their foreign contacts will be acquired under § 1881a.").

7. *Id.* at 1148–49 & n.4.

8. The statute *does* allow "electronic communication service providers" that receive section 702 directives from the government to object via *in camera* proceedings before the FISA Court—and to appeal adverse decisions to the FISA Court of Review and Supreme Court, where necessary. *See* 50 U.S.C. §§ 1881a(h)(4), (6). To date, however, *no* recipient of section 702 directives has availed itself of such an opportunity. *See* Letter from Hon. Reggie B. Walton, Presiding Judge, FISC, to Hon. Patrick J. Leahy, Chairman, Sen. Comm. on the Judiciary, at 8–9 (July 29, 2013), *available at* http://www.leahy.senate.gov/ download/ honorable-patrick-j-leahy.

9. Barton Gellman & Laura Poitras, *U.S., British Intelligence Mining Data from Nine U.S. Internet Companies in Broad Secret Program*, WASH. POST, June 6, 2013, at A1.

10. Barton Gellman & Ashkan Soltani, *NSA Infiltrates Links to Yahoo, Google Data Centers Worldwide, Snowden Documents Say*, WASH. POST, Oct. 30, 2013, at A1; *see also* Barton Gellman et al., *How We Know the NSA Had Access to Internal Google and Yahoo Cloud Data*, WASH. POST, Nov. 4, 2013, http://www.washingtonpost.com/blogs/the-switch/wp/2013/11/04/how-we-know-the-nsa-had-access-to-internal-google-and-yahoo-cloud-data/.

One can certainly question whether *Clapper* would have come out the same way if these stories had broken prior to the Court's decision.[11] And yet, although these disclosures seem to give even greater credence to the plaintiffs' allegations in *Clapper*, they don't necessarily cure the standing defect identified by Justice Alito. After all, plaintiffs still can't identify *specific* communications of theirs that have been obtained by the government under PRISM. Moreover, even in the analogous context of the telephony metadata program under section 215 of the USA PATRIOT Act,[12] where the FISA Court orders disclosed by Edward Snowden included one identifying a specific phone company (Verizon) that has been turning over all of its business customers' metadata,[13] the government has continued to argue that parties don't have standing to challenge such collection unless they can demonstrate not just that the government is *obtaining* their data, but that it is *using* it, as well.[14]

Whatever the merits of these arguments, it remains unlikely as a general matter that the Snowden disclosures, by themselves, will have more than a frictional effect upon the ability of most of those whose communications are intercepted under secret government surveillance programs to challenge such surveillance in court. Instead, the far more interesting question is how the relationship between standing and secret surveillance fits into the reforms Congress is currently considering with regard to improving accountability mechanisms in these contexts. That is to say, does Justice Alito's logic compel the conclusion that Article III prevents Congress from "fixing" *Clapper*, as it were (by relaxing the restrictive standing rule that Justice Alito's majority opinion articulates), or from otherwise providing for more vigorous judicial review of secret

---

11. *See, e.g.*, Steve Vladeck, *The Verizon/Section 215 Order and the* Clapper *Mindset*, LAWFARE, June 5, 2013 (11:00 p.m.) http://www.lawfareblog.com/2013/06/the-verizonsection-215-order-and-the-clapper-mindset/.

12. Uniting and Strengthening America By Providing Appropriate Tools Required To Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001, Pub. L. No. 107-56, § 215, 115 Stat. 272, 287 (codified as amended at 50 U.S.C. § 1861).

13. *See In re* Application of the FBI for an Order Requiring the Production of Tangible Things from Verizon Bus. Network Servs., Inc., No. 13-80 (FISA Ct. Apr. 25, 2013), *available at* http://www.theguardian.com/world/interactive/2013/jun/06/verizon-telephone-data-court-order.

14. *See, e.g.*, Defendants' Memorandum of Law in Support of Motion To Dismiss the Complaint at 11–14, ACLU v. Clapper, No. 13-3994 (S.D.N.Y. filed Aug. 26, 2013) [hereinafter *ACLU* Motion to Dismiss].

surveillance programs?

On the surface, the answer to this question appears to be "yes." Under the Supreme Court's 1992 decision in *Lujan* v. *Defenders of Wildlife*, Congress lacks the power to confer standing upon plaintiffs in cases in which no Article III standing exists.[15] As Justice Scalia wrote for the *Lujan* majority, "Whether the courts were to act on their own, or at the invitation of Congress, in ignoring the concrete injury requirement described in our cases, they would be discarding a principle fundamental to the separate and distinct constitutional role of the Third Branch."[16] But upon closer consideration, *Lujan* is not as clear-cut as it is often portrayed. After all, Justices Kennedy and Souter—whose votes were necessary to the result—saw the issue more narrowly. "In my view," Kennedy wrote for the pair, "Congress has the power to define injuries and articulate chains of causation that will give rise to a case or controversy where none existed before."[17] The key is that "Congress must at the very least identify the injury it seeks to vindicate and relate the injury to the class of persons entitled to bring suit."[18]

In this symposium essay, I aim to explore the implications of Justice Kennedy's broader understanding of Congress's power to confer standing for judicial review of secret surveillance programs going forward. After introducing the *Lujan* and *Clapper* decisions in Part I, Part II turns to one possible implication—that Congress could respond to *Clapper* by expressly lowering the threshold that plaintiffs must surmount in challenges to secret surveillance. As Part II concludes, it probably would not offend the reasoning of Justice Kennedy's *Lujan* concurrence for Congress to authorize challenges to secret surveillance programs so long as plaintiffs could show that there was a "reasonable likelihood" that their communications would be intercepted by the government.

Such a conclusion is without regard to the *merits* of such challenges, of course, but it would suggest that suits like *Clapper* could indeed go forward—allowing courts to reach the difficult statutory and constitutional questions that their merits present. As Part II concludes, though, there are reasons to doubt the long-term utility and efficacy of such a solution, even if its legal validity seems clear.

---

15. 504 U.S. 555 (1992).

16. *Id.* at 576.

17. *Id.* at 580 (Kennedy, J., concurring in part and concurring in the judgment).

18. *Id.* at 576.

With that in mind, Part III considers an alternative possibility—that, instead of empowering individuals like the *Clapper* plaintiffs to bring civil suits challenging secret government surveillance programs (which may very well defeat the purpose of *secret* surveillance), Congress might provide for greater (secret) adversarial process before the FISA Court itself. As Part III explains, such reforms would raise no new Article III concerns in the FISA Court, but would trigger difficult questions about standing to *appeal*—especially after the Supreme Court's decision in the Proposition 8 case.[19] Thus, for policymakers interested in increasing judicial review of secret government surveillance programs, the most logical (if imperfect) course may well be to pursue some combination of *both* measures—allowing parties to sue in those rare cases when information becomes public; and providing for more adversarial process in cases in which it has not.

## I. ARTICLE III STANDING, CONGRESS, AND *CLAPPER*

It is familiar sledding that, throughout the 1970s and 1980s, the Supreme Court read into the case-or-controversy requirement of Article III of the Constitution ever-stricter requirements for establishing standing.[20] Whatever the cause of the shift in the Court's jurisprudence,[21] it was settled doctrine by the end of the 1980s that plaintiffs must establish "injury in fact," "causation," and "redressability" in order to have Article III standing to sue.[22] The one big question that the Justices had yet to answer was how much latitude Congress possessed to *define* those elements, especially when creating federal statutory causes of action for injuries arising under federal law.

### A. *Lujan*: Justice Scalia vs. Justice Kennedy

The Court answered that question in 1992 in *Lujan* v. *Defenders of*

19. *See* Hollingsworth v. Perry, 133 S. Ct. 2652 (2013).

20. *See, e.g.*, William A. Fletcher, *The Structure of Standing*, 98 YALE L.J. 221 (1988); Cass R. Sunstein, *What's Standing After* Lujan*?: Of Citizen Suits, "Injuries," and Article III*, 91 MICH. L. REV. 163 (1992).

21. *See, e.g.*, RICHARD H. FALLON JR. ET AL., HART & WECHSLER'S THE FEDERAL COURTS AND THE FEDERAL SYSTEM 114 (6th ed. 2009) (summarizing competing "sources of strain" that may have helped to precipitate modern standing doctrine).

22. *See, e.g.*, Allen v. Wright, 468 U.S. 737 (1984).

*Wildlife*.[23] At issue was the citizen-suit provision of the Endangered Species Act of 1973, which provided that "any person may commence a civil suit on his own behalf . . . to enjoin any person, including the United States and any other governmental instrumentality or agency . . . who is alleged to be in violation of any provision of this chapter."[24] In *Lujan*, a host of environmental groups invoked that provision to challenge a new federal regulation that rescinded the applicability of various ESA procedural requirements to new federal projects overseas.

Writing for a 6-3 majority,[25] Justice Scalia first rejected the argument that plaintiffs had alleged an "injury in fact" sufficient to satisfy Article III. As he explained, the plaintiffs had failed to show that any of their members were specifically planning to *visit* the overseas facilities where the new regulation would have had the allegedly deleterious effect, and so could not demonstrate that they were likely to incur a concrete injury as a result of the challenged administrative action. For a four-Justice plurality, Scalia also concluded that the plaintiffs had failed to satisfy Article III's redressability requirement: "Instead of attacking the separate decisions to fund particular projects allegedly causing them harm, respondents chose to challenge a more generalized level of Government action (rules regarding consultation), the invalidation of which would affect all overseas projects."[26]

But the heart of Justice Scalia's opinion was Part IV, in which he explained (at least formally for the majority) that the citizen-suit provision of the ESA could not constitutionally cure either of these defects. As he wrote,

> there is absolutely no basis for making the Article III inquiry turn on the source of the asserted right. Whether the courts were to act on their own, or at the invitation of Congress, in ignoring the concrete injury requirement described in our cases, they would be discarding a principle

23. 504 U.S. 555.

24. 16 U.S.C. § 1540(g)(1)(A).

25. Although seven Justices joined in the judgment, Justice Stevens did so only on the merits; like the dissenters, he disagreed with the majority's conclusion that the plaintiffs lacked standing to proceed. *See Lujan*, 504 U.S. at 581–82 (Stevens, J., concurring in the judgment); *id.* at 589–606 (Blackmun, J., dissenting).

26. *Id.* at 568 (plurality opinion).

> fundamental to the separate and distinct constitutional role of the Third Branch—one of the essential elements that identifies those "Cases" and "Controversies" that are the business of the courts rather than of the political branches.[27]

*Lujan* thereby held that Congress had violated Article III in the ESA by purporting to confer standing upon those who could not satisfy the Court's three-pronged interpretation of the Constitution's case-or-controversy requirement. To be sure, Justice Scalia concluded, "[Statutory] broadening [of] the categories of injury that may be alleged in support of standing is a different matter from abandoning the requirement that the party seeking review must himself have suffered an injury."[28] But even in the former set of cases, Justice Scalia's opinion for the *Lujan* Court appeared to portend fairly sharp limits on Congress's power to so provide.[29]

And yet, although Part IV of Justice Scalia's opinion in *Lujan* was nominally for a six-Justice majority, Justice Kennedy's concurring opinion—in which Justice Souter joined in full—offered a somewhat narrower understanding of the constitutional limits that the case-or-controversy requirement imposes on Congress.[30] Justice Kennedy agreed that it would violate Article III "if, at the behest of Congress and in the absence of any showing of concrete injury, we were to entertain citizen suits to vindicate the public's nonconcrete interest in the proper administration of the laws."[31] At the same time, he was equally clear that, "As Government programs and policies become more complex and

---

27. *Id.* at 576 (majority opinion).

28. *Id.* at 578 (quoting Sierra Club v. Morton, 405 U.S. 727, 738 (1972)) (alterations in original).

29. In an influential speech, then-Judge Scalia had already previewed his view of the strict limits that the Constitution imposes on Congress's power to confer standing. *See* Antonin Scalia, *The Doctrine of Standing as an Essential Element of the Separation of Powers*, 17 SUFFOLK U. L. REV. 881 (1983).

30. *Lujan*, 504 U.S. at 579–81 (Kennedy, J., concurring in the judgment). With respect to Part IV of Justice Scalia's opinion, Kennedy flagged that he joined it "with the following observations." *Id.* at 580; *see also, e.g.*, Amason v. Kangaroo Exp., No. 09-2117, 2013 WL 987935, at 3 n.5 (N.D. Ala. Mar. 11, 2013) ("Because a majority opinion in *Lujan* is made possible only by counting Justice Kennedy's concurrence, its consideration is important in interpreting the holding of *Lujan*.").

31. *Lujan*, 504 U.S. at 580–81.

farreaching, we must be sensitive to the articulation of new rights of action that do not have clear analogs in our common-law tradition."[32] Unlike the general skepticism of broad statutory standing provisions evinced by Justice Scalia, the key for Justice Kennedy was that "the party bringing suit must show that the action injures him in a concrete and personal way."[33] Thus, the upshot of Justice Kennedy's concurring opinion was that Congress *did* have fairly wide discretion to create an injury sufficiently concrete to satisfy Article III where one previously had not existed; it had just exceeded its limits in the ESA.

### B. After *Lujan*

Although the distinction between Justice Scalia's majority opinion and Justice Kennedy's concurrence may at first have appeared semantic, the Court's subsequent jurisprudence illuminated both that (1) there truly *is* daylight between Justice Kennedy's and Justice Scalia's view of Congress's power to confer standing; and (2) *Lujan* was an exceptionally rare case in which Congress exceeded the wide latitude Justice Kennedy believes it possesses to confer standing upon plaintiffs who might not otherwise be entitled to sue to vindicate certain statutory and constitutional injuries.

For example, in *FEC* v. *Akins*,[34] Justice Breyer (writing for a 6-3 majority that included Justice Kennedy) found no Article III problem with the Federal Election Campaign Act of 1971 (FECA),[35] even though it authorized *any* person to challenge alleged violations of the statute in the Federal Election Commission, and then to bring suit if the FEC dismissed their complaint.[36] In *Akins*, the plaintiffs challenged the FEC's determination that the American-Israel Public Affairs Committee (AIPAC) was not a "political committee," and was therefore not required to comply with various disclosure regulations and public reporting requirements.[37] Notwithstanding a sharply worded dissent from Justice

32. *Id.* at 580.

33. *Id.* at 581.

34. 524 U.S. 11 (1998).

35. Pub. L. No. 92-225, 86 Stat. 3 (codified as amended at 2 U.S.C. §§ 431–457).

36. *See* 2 U.S.C. § 437g(a)(1), (a)(8)(A).

37. *See id.* § 431(4)(a).

Scalia,[38] the Court held that "the informational injury at issue here, directly related to voting, the most basic of political rights, is sufficiently concrete and specific such that the fact that it is widely shared does not deprive Congress of constitutional power to authorize its vindication in the federal courts."[39]

Two years later, the Court in *Friends of the Earth, Inc.* v. *Laidlaw Environmental Services (TOC), Inc.* upheld the standing of environmental plaintiffs who brought suit under the citizen-suit provision of the Clean Water Act[40] claiming that a permitted business was violating the Act's mercury discharge limits.[41] Focusing on the distinction between "injury to the environment" and "injury to the plaintiff,"[42] Justice Ginsburg's majority opinion highlighted the injuries alleged by various of Friends of the Earth's members.[43] Because these injuries were concrete and specific, the Court held that they were sufficient to satisfy Article III standing.[44]

In a short concurrence, Justice Kennedy flagged the "[d]ifficult and fundamental questions [that] are raised when we ask whether exactions of public fines by private litigants, and the delegation of Executive power which might be inferable from the authorization, are permissible in view of the responsibilities [constitutionally] committed to the Executive."[45] But he nevertheless joined the majority, as opposed to Justice Scalia's dissent, which concluded that "[t]he undesirable and unconstitutional consequence of today's decision is to place the immense power of suing to enforce the public laws in private hands."[46]

Finally, in *Massachusetts* v. *EPA*,[47] a 5-4 majority (again including Justice Kennedy) held that a state had standing to sue the Environmental Protection Agency under the Clean Air Act to challenge its failure to

38. *See, e.g.*, *Akins*, 514 U.S. at 29–30 (Scalia, J., dissenting) ("The provision of law at issue in this case is an extraordinary one, conferring upon a private person the ability to bring an Executive agency into court to compel its enforcement of the law against a third party.").

39. *Id.* at 24–25 (majority opinion).

40. 33 U.S.C. § 1365(a).

41. 528 U.S. 167 (2000).

42. *Id.* at 181.

43. *See id.* at 181–83.

44. *See id.* at 183–88.

45. *Id.* at 197 (Kennedy, J., concurring).

46. *Id.* at 215 (Scalia, J., dissenting).

47. 549 U.S. 497 (2007).

regulate greenhouse gas emissions from motor vehicles.[48] Although some elements of Justice Stevens's analysis appeared to turn on the "special solicitude" owed to states as plaintiffs,[49] Justice Stevens also emphasized the critical role of Congress—citing to Justice Kennedy's view thereof: "The parties' dispute turns on the proper construction of a congressional statute, a question eminently suitable to resolution in federal court. Congress has moreover authorized this type of challenge to EPA action. That authorization is of critical importance to the standing inquiry."[50] Notwithstanding a stern dissent from Chief Justice Roberts (joined by, among others, Justice Scalia), the Court therefore allowed Massachusetts' challenge to go forward.[51]

To be sure, as the Court's most recent environmental standing case—*Summers* v. *Earth Island Institute*[52]—attests, Justices Scalia and

48. *See* 42 U.S.C. § 7607(b)(1) (authorizing judicial review of "any . . . nationally applicable regulations promulgated, or final action taken, by the Administrator").

49. *See* Stephen I. Vladeck, *States' Rights and State Standing*, 46 U. RICH. L. REV. 845, 856–57 (2012) (situating *Massachusetts* within a broader array of decisions in which the Supreme Court has recognized state standing when states are suing to enforce *their* federal rights, as opposed to the rights of their citizens).

50. *Massachusetts*, 549 U.S. at 516 (citation omitted). The remainder of the paragraph (and most of the next page) quoted from Justice Kennedy's *Lujan* concurrence. *See id.* at 516–17 (quoting Lujan v. Defenders of Wildlife, 504 U.S. 555, 580 (Kennedy , J., concurring in part and concurring in judgment)).

51. *Id.* at 535–49 (Roberts, C.J., dissenting). Justice Scalia penned a separate dissent—albeit on the merits. *See id.* at 549–60 (Scalia, J., dissenting).

52. 555 U.S. 488 (2009). Specifically, *Summers* held that environmental organizations lacked standing to sue the U.S. Forest Service in order to enjoin application of regulations to exempt certain timber from the notice, comment, and appeal process set forth in the Forest Service Decisionmaking and Appeals Reform Act. Although the Act authorized such claims, Justice Scalia's majority opinion stressed that

> It makes no difference that the procedural right has been accorded by Congress. That can loosen the strictures of the redressability prong of our standing inquiry—so that standing existed with regard to the Burnt Ridge Project, for example, despite the possibility that Earth Island's allegedly guaranteed right to comment would not be successful in persuading the Forest Service to avoid impairment of Earth Island's concrete interests. Unlike redressability, however, the requirement of injury in fact is a hard floor of Article III jurisdiction that cannot be removed by statute.

*Id.* at 497 (citations omitted).

Kennedy are still often on the same side in Article III standing cases, even those raising Congress's power to create standing where none previously existed. But even in *Summers*, Justice Kennedy wrote a separate concurrence to explain that he was joining Justice Scalia's majority opinion only because he agreed that "deprivation of a procedural right without some concrete interest that is affected by the deprivation—a procedural right *in vacuo*—is insufficient to create Article III standing."[53] As he elaborated, "This case would present different considerations if Congress had sought to provide redress for a concrete injury 'giv[ing] rise to a case or controversy where none existed before.' Nothing in the statute at issue here, however, indicates Congress intended to identify or confer some interest separate and apart from a procedural right."[54]

*Akins*, *Friends of the Earth*, *Massachusetts*, and *Summers* all dealt with Congress's power to define "injuries" on terms more capacious than those courts would otherwise have identified, and not Congress's power to define the burden of proof plaintiffs must satisfy in order to *establish* an injury in fact. But Justice Kennedy's *Lujan* concurrence stressed Congress's power to *both* "define injuries *and* articulate chains of causation that will give rise to a case or controversy where none existed before." It should follow that Congress's power to articulate chains of causation includes Congress's power to legislate the means pursuant to which plaintiffs may demonstrate that such chains exist. There has not yet been a post-*Lujan* case testing this proposition, however—perhaps because Congress has not been impelled to so provide in any post-*Lujan* statute.

### C. *Clapper*

Unlike the cases surveyed above, the lawsuit that gave rise to the Supreme Court's *Clapper* decision was not seeking to take advantage of a citizen-suit provision. Instead, *Clapper* involved a fairly conventional constitutional challenge to an unconventional statute—the FISA Amendments Act of 2008.[55] The origins and history of the FAA have been

53. *Id.* at 501 (Kennedy, J., concurring) (internal quotation marks omitted).

54. *Id.* (quoting *Lujan*, 504 U.S. at 580 (Kennedy, J., concurring in part and concurring in the judgment) (alteration in original)).

55. Foreign Intelligence Surveillance Act Amendments Act of 2008, Pub. L. No. 110-261, § 101, 122 Stat. 2436, 2438–48 (codified at 50 U.S.C. §§ 1881–1881g).

well-described elsewhere;[56] for present purposes, it suffices to highlight the FAA's centerpiece, new section 702 of FISA. As Justice Alito summarized in *Clapper*, that provision

> supplements pre-existing FISA authority by creating a new framework under which the Government may seek the FISC's authorization of certain foreign intelligence surveillance targeting the communications of non-U.S. persons located abroad. Unlike traditional FISA surveillance, § 1881a does not require the Government to demonstrate probable cause that the target of the electronic surveillance is a foreign power or agent of a foreign power. And, unlike traditional FISA, § 1881a does not require the Government to specify the nature and location of each of the particular facilities or places at which the electronic surveillance will occur.[57]

Section 702 makes clear that the authorized surveillance cannot be undertaken with the intent or purpose of targeting U.S. persons.[58] But insofar as section 702 contemplates the sweeping and undifferentiated interception of a high volume of electronic communications, it is certainly at least possible—if not likely—that communications of U.S. persons will be intercepted notwithstanding such statutory constraints.

With that in mind, a group of plaintiffs who routinely communicate with non-citizens outside the United States brought suit on the day the FISA Amendments Act was signed into law, challenging section 702 on a host of constitutional grounds. Foremost among these was the claim that the statute violated the Fourth Amendment insofar as it authorized the *knowing* interception of U.S. persons' communications without a warrant and/or probable cause.[59] And because fear of such interception had led the

---

56. *See, e.g.*, 1 DAVID KRIS & J. DOUGLAS WILSON, NATIONAL SECURITY INVESTIGATIONS AND PROSECUTIONS §§ 9:11, 17:3 (2d ed. 2012); *see also* Stephanie Cooper Blum, *What Really is at Stake With the FISA Amendments Act of 2008 and Ideas for Future Surveillance Reform*, 18 B.U. PUB. INT. L.J. 269 (2009).

57. Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138, 1144 (2013) (citations omitted).

58. *See* 50 U.S.C. § 1881a(b).

59. To be clear, the Fourth Amendment argument is hardly open-and-shut. The FISA Court of Review, for example, has recognized a "foreign intelligence surveillance" exception to the Fourth Amendment's Warrant Clause, *see In re* Directives [Redacted] Pursuant to

plaintiffs to take concrete steps to communicate through alternative channels, they claimed that section 702 thereby caused an "injury-in-fact" sufficient to confer Article III standing.[60]

In August 2009, the U.S. District Court for the Southern District of New York disagreed.[61] Relying on an earlier Sixth Circuit decision concluding that similar plaintiffs lacked standing to challenge the warrantless "Terrorist Surveillance Program,"[62] Judge Koeltl held that Article III standing was absent because section 702 did not (1) directly regulate or proscribe the plaintiffs' conduct; or (2) authorize surveillance of a class of persons that included the plaintiffs.[63]

Eighteen months later, the Second Circuit reversed.[64] As Judge Lynch wrote for a unanimous three-judge panel,

> the plaintiffs here have alleged that they reasonably anticipate direct injury from the enactment of the FAA because, unlike most Americans, they engage in legitimate professional activities that make it reasonably likely that their privacy will be invaded and their conversations overheard—unconstitutionally, or so they argue—as a result of the surveillance newly authorized by the FAA, and that they have already suffered tangible, indirect injury due to the reasonable steps they have undertaken to avoid such overhearing, which would impair their ability to carry out

---

Section 105B of the Foreign Intelligence Surveillance Act, 551 F.3d 1004 (FISA Ct. Rev. 2008), which, if valid, would arguably encompass *all* surveillance conducted under section 702. Even if such an exception does not encompass interception of U.S. persons' communications, courts have held in other contexts that the "incidental" interception of protected communications as part of otherwise valid surveillance does not violate the Fourth Amendment. *But see* United States v. Bin Laden, 126 F. Supp. 2d 264, 280–82 (S.D.N.Y. 2000) (questioning the applicability of this rule in cases in which the "incidental" interception is not unanticipated).

60. *See* Complaint for Declaratory and Injunctive Relief, Amnesty Int'l USA v. McConnell, 646 F. Supp. 2d 633 (S.D.N.Y. 2009) (No. 08-civ-6259), *available at* https://www.aclu.org/files/pdfs/natsec/amnesty/07_10_2008_Complaint.pdf.

61. *McConnell*, 646 F. Supp. 2d 633.

62. *See* ACLU v. NSA, 493 F.3d 644 (6th Cir. 2007).

63. *McConnell*, 646 F. Supp. 2d at 645–58.

64. Amnesty Int'l USA v. Clapper, 638 F.3d 118 (2d Cir. 2011).

those activities.[65]

The government subsequently sought rehearing en banc, only to have the Second Circuit divide 6-6.[66] Granting the government's ensuing petition for certiorari,[67] the Supreme Court reversed the Second Circuit, holding that the plaintiffs had failed to carry the Article III standing burden.[68]

As noted above, at the heart of Justice Alito's opinion for a 5-4 majority in *Clapper* was the plaintiffs' inability to show that their communications were being (or would be) intercepted pursuant to surveillance undertaken under section 702. As he explained,

> Respondents assert that they can establish injury in fact that is fairly traceable to § 1881a because there is an objectively reasonable likelihood that their communications with their foreign contacts will be intercepted under § 1881a at some point in the future. This argument fails. As an initial matter, the Second Circuit's "objectively reasonable likelihood" standard is inconsistent with our requirement that "threatened injury must be certainly impending to constitute injury in fact." Furthermore, respondents' argument rests on their highly speculative fear that: (1) the Government will decide to target the communications of non-U.S. persons with whom they communicate; (2) in doing so, the Government will choose to invoke its authority under § 1881a rather than utilizing another method of surveillance; (3) the Article III judges who serve on the Foreign Intelligence Surveillance Court will conclude that

65. *Id.* at 149.

66. Amnesty Int'l USA v. Clapper, 667 F.3d 163 (2d Cir. 2011) (mem.). The six dissenting judges penned four separate opinions explicating their reasons for dissenting from the denial of rehearing en banc. *See id.* at 172 (Raggi, J., dissenting from denial of rehearing en banc); *id.* at 193 (Livingston, J., dissenting from denial of rehearing en banc); *id.* at 200 (Jacobs, C.J., dissenting from denial of rehearing en banc); *id.* at 204 (Hall, J., dissenting from denial of rehearing en banc). The dissents prompted a concurrence from Judge Lynch—the author of the panel opinion and the only member of the panel entitled to participate in the en banc proceedings. *See id.* at 164 (Lynch, J., concurring in the denial of rehearing en banc).

67. Clapper v. Amnesty Int'l USA, 132 S. Ct. 2431 (2012) (mem.).

68. Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138 (2013).

> the Government's proposed surveillance procedures satisfy § 1881a's many safeguards and are consistent with the Fourth Amendment; (4) the Government will succeed in intercepting the communications of respondents' contacts; and (5) respondents will be parties to the particular communications that the Government intercepts. As discussed below, respondents' theory of standing, which relies on a highly attenuated chain of possibilities, does not satisfy the requirement that threatened injury must be certainly impending.[69]

Of course, the only reason why the plaintiffs' allegations in this regard were so "highly speculative" was because the government's surveillance operations under section 702 were (and largely remain) secret. As Justice Breyer pointed out in his dissent, the surveillance alleged by the plaintiffs "is as likely to take place as are most future events that commonsense inference and ordinary knowledge of human nature tell us will happen."[70] In any event, the real flaw with the majority opinion, Breyer argued, was its adoption of the "certainly impending" standard. In his words, "*certainty* is not, and never has been, the touchstone of standing. The future is inherently uncertain." Instead, "what the Constitution requires is something more akin to 'reasonable probability' or 'high probability.' The use of some such standard is all that is necessary here to ensure the actual concrete injury that the Constitution demands."[71]

### D. After *Clapper* (and Snowden)

The Supreme Court's decision in *Clapper* may well have sounded the death knell for suits challenging secret surveillance, but for the

---

69. *Id.* at 1147–48 (citations omitted).

70. *Id.* at 1155 (Breyer, J., dissenting); *see also id.* at 1160 ("[W]e need only assume that the Government is doing its job (to find out about, and combat, terrorism) in order to conclude that there is a high probability that the Government will intercept at least some electronic communication to which at least some of the plaintiffs are parties. The majority is wrong when it describes the harm threatened plaintiffs as 'speculative.'").

71. *Id.* at 1165; *see also id.* at 1160 ("[F]ederal courts frequently entertain actions for injunctions and for declaratory relief aimed at preventing future activities that are reasonably likely or highly likely, but not absolutely certain, to take place. And that degree of certainty is all that is needed to support standing here.").

disclosures by former NSA employee Edward Snowden that began in June 2013. One of Snowden's most significant leaks was the existence and scope of the so-called "PRISM" program, ostensibly undertaken pursuant to section 702. Quoting Oregon Senator Mark Udall, the front-page *Washington Post* article disclosing the program noted that "there is nothing to prohibit the intelligence community from searching through a pile of communications, which may have been incidentally or accidentally been collected without a warrant, to deliberately search for the phone calls or e-mails of specific Americans."[72]

Together with later disclosures,[73] the PRISM story appears to indicate that the surveillance of which the plaintiffs complained in *Clapper was* "certainly impending"; indeed, it was already afoot. In light of *Clapper*, the question then turned to how such surveillance might be subjected to greater judicial review.

## II. THE *CLAPPER* "FIX"?: LOWERING THE STANDING BAR BY STATUTE

### A. FISA After *Clapper*

Notwithstanding Snowden's disclosures, the government has continued to argue in analogous contexts that the Supreme Court's *Clapper* decision militates against standing to challenge the government's secret surveillance programs. Thus, in the ACLU's challenge to the bulk metadata collection program under section 215 of the USA PATRIOT Act, the government has continued to contest standing despite the disclosure of orders by the FISA Court compelling telephone companies like Verizon to turn over their business customers' telephony metadata in bulk. Specifically, the government's argument is that the alleged constitutional violation—and, therefore, the Article III injury—does not arise from the *collection* of the metadata, but only from its querying. And because plaintiffs can only demonstrate that their metadata are being collected (and not that they are being queried), they cannot overcome *Clapper*.[74]

Whatever one thinks of such a distinction as a logical matter, the

72. Gellman & Poitras, *supra* note 9; *see also id.* ("Even when the system works just as advertised, with no American singled out for targeting, the NSA routinely collects a great deal of American content. That is described as 'incidental,' and it is inherent in contact chaining, one of the basic tools of the trade.").

73. *See supra* note 10 and accompanying text.

74. *See ACLU* Motion to Dismiss, *supra* note 14.

larger legal point that it underscores is the exceptionally high bar *Clapper* imposes before plaintiffs will be able to challenge secret government surveillance programs going forward. Indeed, even if courts subsequently conclude, contra the government, that the injury occurs at the point of collection, that still assumes that future plaintiffs will be able to *prove* that such collection is occurring—a difficult proposition at best in the absence of additional Snowden-like disclosures.

At the same time, one of the more underappreciated features of FISA is the cause of action it already provides for an "aggrieved person" "other than a foreign power or an agent of a foreign power [as defined by FISA], who has been subjected to an electronic surveillance."[75] FISA defines "electronic surveillance" somewhat convolutedly,[76] but it nevertheless manifests Congress's intent, from the inception of FISA, to allow those whose communications are unlawfully obtained *under* FISA to bring private suits to challenge such surveillance.[77] Simply put, Congress has already *created* a private cause of action for FISA suits; it has just never clarified how putative plaintiffs can demonstrate that they are, in fact, "aggrieved persons."

## B. Defining the Injury

With that in mind, suppose Congress enacted the following language as new subsection (b) to 50 U.S.C. § 1810:

> For purposes of any claim brought in any court of the United States challenging surveillance conducted pursuant to this chapter, an "aggrieved person" is any person or entity (other than a foreign power or an agent of a foreign power) who can demonstrate (1) a reasonable basis to believe that

75. 50 U.S.C. § 1810; *see also* Fed. Elec. Comm'n v. Akins, 524 U.S. 11, 19 (1998) ("History associates the word 'aggrieved' with a congressional intent to cast the standing net broadly—beyond the common-law interests and substantive statutory rights upon which "prudential" standing traditionally rested.").

76. *See* 50 U.S.C. § 1801(f).

77. In *Al-Haramain Islamic Foundation, Inc.* v. *Obama*, 705 F.3d 845 (9th Cir. 2012), the Ninth Circuit held that Congress, in creating the cause of action provided by § 1810, was insufficiently clear that it intended to waive the federal government's sovereign immunity, and so § 1810 did not authorize suits for damages. Leaving aside the questionable logic of the court's analysis, it does not disturb the availability of § 1810 for suits for declaratory or injunctive relief.

> their communications will be acquired under this chapter; and (ii) that they have taken objectively reasonable steps to avoid such surveillance.[78]

At first blush, such language should largely ameliorate the *Clapper* problem. After all, one can hardly conclude that the *Clapper* plaintiffs' concerns were *unreasonable* given the language of the statute as it was enacted—and especially after and in light of the *Washington Post*'s Snowden-aided disclosure of the PRISM program. To similar effect, the *Clapper* plaintiffs had indeed undertaken objectively reasonable steps to avoid such surveillance—by pursuing alternative (and more expensive) means of communicating with non-citizens outside the territorial United States.[79] Indeed, it should not even be a close question whether the *Clapper* plaintiffs could satisfy such a statutory standing provision.

The harder question is whether such language would be constitutional. In his *Clapper* dissent, Justice Breyer seemed to suggest that the answer would be yes: "[W]hat the Constitution requires is something more akin to 'reasonable probability' or 'high probability.' The use of some such standard is all that is necessary here to ensure the actual concrete injury that the Constitution demands."[80] And, per the above discussion, Justice Kennedy's *Lujan* concurrence and subsequent opinions appear to support Justice Breyer's view inasmuch as they underscore his view of Congress's power to "articulate chains of causation." So long as Congress is not creating standing for what is (1) effectively a generalized grievance;[81] or

78. For an earlier variation on this theme, see Steve Vladeck, *The* Clapper *Fix: Congress and Standing to Challenge Secret Surveillance*, LAWFARE, June 20, 2013 (12:48 p.m.), http://www.lawfareblog.com/2013/06/the-clapper-fix-congress-and-standing-to-challenge-secret-surveillance/.

79. *See, e.g.*, Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138, 1145–46 (2013).

80. *Id.* at 1168 (Breyer, J., dissenting).

81. For potentially nationwide surveillance such as the bulk metadata and PRISM programs, it is certainly true that any constitutional "injury" is widely shared. Standing alone, though, that fact does not raise generalized grievance concerns: "Often the fact that an interest is abstract and the fact that it is widely shared go hand in hand. But their association is not invariable, and where a harm is concrete, though widely shared, the Court has found 'injury in fact.'" Fed. Elec. Comm'n v. Akins, 524 U.S. 11, 24 (1998) (citing Public Citizen v. U.S. Dep't of Justice, 491 U.S. 440, 449–50 (1989)).

(2) a procedural right without a substantive deprivation,[82] Justice Kennedy appears to share the view of the *Clapper* dissenters—and would therefore likely uphold such a potentially expansive standing provision.

### C. The Potential Shortcomings of a *Clapper* Fix

Ultimately, the larger problems with such a *Clapper* "fix" are not legal, but practical: For starters, there is little reason to believe that disclosures of programs such as PRISM are going to become a recurring feature of American public discourse—or even that we now know about all of the potentially unlawful secret surveillance to which U.S. persons are currently subjected. And to the extent that current or future programs are based upon statutes not remotely as clear in their potential scope as section 702, the absence of such disclosures would necessarily be fatal to the ability of plaintiffs to satisfy even the lower standing threshold proposed above. Simply put, such a *Clapper* fix may well be constitutional, but it may also not accomplish all that much outside the specific context of challenges to section 702.

The same logic would also presumably result if the government succeeds in its efforts to distinguish between the *collection* of information from U.S. persons and the querying of that information, an argument that has been publicly aired only in a district court brief thus far.[83] If the relevant injury for constitutional purposes does not arise from the government's obtaining of an individual's data and/or communications, but rather its specific accessing thereof, even the language outlined above may well prove inadequate to allow a putative plaintiff to establish that a current or future secret surveillance program is in fact injuring them.

Finally, there is the matter of the elephant in the room: it would logically defeat the purpose of secret surveillance programs if those programs could be challenged in visible, public litigation in which plaintiffs could presumably seek to discover information concerning the existence and scope—and sources and methods—of the government's surveillance. Whether or not the government would be entitled to avail

82. Where the claim is unlawful interception of the *plaintiff*'s communications, this concern is not presented. It *does* arise, however, in the context of allowing other parties to challenge government surveillance programs at least nominally on the public's behalf. *See infra* Part III.

83. *See ACLU* Motion to Dismiss, *supra* note 14.

itself of the state secrets privilege in such cases,[84] the possibility of such disclosure-through-litigation provides still further reason to doubt that "fixing" *Clapper* is a workable, complete, and comprehensive solution.

## III. AN ALTERNATIVE: SPECIAL ADVOCATES AND APPELLATE STANDING

### A. FISA's "Adversarial" Process

The inadequacies of external civil litigation may help to explain why so much attention has increasingly come to focus on the procedures before the FISA Court itself—especially the possibility of improving upon and expanding mechanisms for adversarial participation before the court as a means of increasing accountability for secret government surveillance programs.[85] This point may seem counterintuitive; as initially conceived, FISA was designed explicitly to *not* be adversarial, but to instead resemble the *ex parte* and *in camera* warrant process Congress codified in the context of wiretap applications in ordinary criminal cases.[86] Indeed, the lack of adversarial process led some—including future Court of Appeals (and FISA Court of Review) Judge Laurence Silberman—to argue that such proceedings might even violate Article III insofar as they effectively sought advisory opinions from the FISA Court.[87]

---

84. At least one district court has held that the cause of action provided by FISA, *see* 50 U.S.C. § 1810, necessarily abrogates the state secrets privilege in cases brought under that provision. *See In re* Nat'l Security Agency Telecomms. Records Litig., 700 F. Supp. 2d 1182 (N.D. Cal. 2010), *aff'd in part, rev'd in part on other grounds sub nom.* Al-Haramain Islamic Found. v. Obama, 705 F.3d 845 (9th Cir. 2012). The Fourth Circuit, in contrast, has held that the state secrets privilege is constitutionally grounded, *see* El-Masri v. United States, 479 F.3d 296, 303 (4th Cir. 2007) ("Although the state secrets privilege was developed at common law, it performs a function of constitutional significance, because it allows the executive branch to protect information whose secrecy is necessary to its military and foreign-affairs responsibilities."), which would seem to militate against Congress's power to abrogate it.

85. *See, e.g.*, James G. Carr, *A Better Secret Court*, N.Y. TIMES, July 23, 2013, at A21; *see also, e.g.*, Stephen I. Vladeck, *It's Time To Fix the FISA Court (the Way Congress Intended)*, MSNBC, Aug. 1, 2013, http://www.msnbc.com/msnbc/its-time-fix-the-fisa-court-the-way.

86. *See, e.g.*, United States v. Koyomejian, 946 F.2d 1450, 1456 (9th Cir. 1991) ("[I]n drafting FISA Congress used Title III as its model, particularly for procedures relating to necessity and minimization."); *see also* S. REP. NO. 95-604 (1978), *reprinted in* 1978 U.S.C.C.A.N. 3904.

87. See *Foreign Intelligence Electronic Surveillance: Hearings on H.R. 5794, 9745, 7308, and 5632 Before the Subcomm. on Legislation of the Permanent Select Comm. on Intelligence*, 95th Cong., 2d Sess.

In ordinary criminal cases, federal courts have long upheld the non-adverse nature of warrant applications by indulging something of a fiction—that the warrants are ancillary to a judicial process that will *eventually* culminate in an opportunity for adversarial presentation of the issues, *e.g.*, in a motion to suppress the fruits of the warrant during a criminal trial, or a civil suit for damages challenging the legality of the search conducted pursuant to the warrant.[88] Insofar as the FISA process was at least initially modeled on a similar understanding, then, the argument goes that FISA satisfies Article III to the same extent as the warrant process in ordinary criminal cases.[89]

Even if that analogy works, though, it fails to account for the fundamental shift in the nature of the judicial review the FISA Court conducts under the government's newer FISA authorities. For example, neither the production orders the government may obtain under section 215 of the USA PATRIOT Act nor the directives that issue under section 702 are even plausibly characterized as "warrants." Nor is it plausible (let

---

221–23 (1978) (statement of Laurence H. Silberman). *See generally* ANDREW NOLAN ET AL., CONG. RES. SERV., INTRODUCING A PUBLIC ADVOCATE INTO THE FOREIGN INTELLIGENCE SURVEILLANCE ACT'S COURTS: SELECT LEGAL ISSUES 19 (2013) (summarizing the constitutional issues surrounding FISA), *available at* http://justsecurity.org/wp-content/uploads/2013/10/CRS-Report-FISC-Public-Advocate-Oct.-25-2013.pdf.

88. *See, e.g.*, David J. Barron & Martin S. Lederman, *The Commander in Chief at the Lowest Ebb—A Constitutional History*, 121 HARV. L. REV. 941, 1106 n.663 (2008).

89. *See, e.g.*, United States v. Megahey, 553 F. Supp. 1180, 1196 (E.D.N.Y. 1982); *see also* United States v. Falvey, 540 F. Supp. 1306, 1313 n.16 (E.D.N.Y. 1982).

A different argument, and one offered by the FISA Court of Review in 2002, is that the judges of the FISA Court are not actually exercising judicial power *at all* when they are approving government applications, and so are not bound by Article III's case-or-controversy requirement. *See, e.g.*, *In re* Sealed Case, 310 F.3d 717, 732 n.19 (FISA Ct. Rev. 2002); *see also* NOLAN ET AL., *supra* note 87, at 16–17. Such an argument utterly fails to persuade. For starters, the FISA Court has itself *held* that it is an Article III court. *See In re* Motion for Release of Court Records, 526 F. Supp. 2d 484, 486 (FISA Ct. 2007) ("Notwithstanding the esoteric nature of its caseload, the FISC is an inferior federal court established by Congress under Article III."); *see also* United States v. Cavanagh, 807 F.2d 787, 791–92 (9th Cir. 1987) (Kennedy, J.). Moreover, its decisions are subject to supervisory *appellate* review by the FISA Court of Review and then the U.S. Supreme Court. Insofar as the FISA process could be justified as existing outside of Article III, having "initial" Article III review in the U.S. Supreme Court would appear to contravene the limits on that Court's original jurisdiction as articulated in *Marbury* v. *Madison*, 5 U.S. (1 Cranch) 137 (1803).

alone likely) that a statistically significant percentage of the information obtained under these authorities will ever be subject to collateral attack in a criminal or civil proceeding. Perhaps because the adverseness fiction breaks down in these contexts, the statutes creating these authorities also provide—for the first time—for the possibility of adverse litigation before the FISA Court.

To that end, section 215 authorizes "[a] person receiving a production order" under that provision to "challenge the legality of that order,"[90] and to seek review in the FISA Court of Review (and, ultimately, in the Supreme Court), if they are unsuccessful.[91] And section 702 authorizes "[a]n electronic communication service provider receiving a directive" under section 702 to "file a petition to modify or set aside such directive with the Foreign Intelligence Surveillance Court,"[92] on the grounds that "the directive does not meet the requirements of this section, or is otherwise unlawful."[93] As with section 215, section 702 further authorizes appeal to the FISA Court of Review, and then the Supreme Court, of adverse decisions.[94]

Both sections also include a panoply of procedural rules in such cases—designed to ensure both the expediency and secrecy of such adversarial process.[95] Presumably, the animating principle behind both provisions is that such adversarial participation can simultaneously (1) ameliorate the Article III questions that FISA might otherwise raise; and (2) allow for at least some adversarial presentation and argument on the relevant legal principles.

One can certainly question *whether* the recipients of directives under section 702 or production orders under section 215 are in a position meaningfully to vindicate the rights of those whose communications are actually being acquired as a result.[96] But there is an even more basic

90. 50 U.S.C. § 1861(f)(2)(A).

91. *Id.* § 1861(f)(3).

92. *Id.* § 1881a(h)(4)(A).

93. *See id.* § 1881a(h)(4)(C).

94. *See id.* § 1881a(h)(6).

95. *See id.* §§ 1861(f)(4), (5), 1881a(h)(4)(D)–(F).

96. Indeed, the interests of a telephone or internet service provider will necessarily diverge from the interests of at least some of their customers, especially given that (1) the provider's cooperation with the government is ostensibly secret; and (2) *non*-cooperation will potentially incur significant economic (and non-economic) costs arising out of the litigation,

problem: According to a July 2013 letter from Judge Walton to the Senate Judiciary Committee,[97] *no* third-party has ever availed themselves of either of these adversarial processes—under section 215 *or* section 702.[98] Thus, even if recipient-based adversarial process *could* provide a sufficient check on secret government surveillance programs, at least thus far, it clearly has not done so.

## B. The "Special Advocate" Proposals

This shortcoming may help to explain the growing support for proposals to have some kind of "special advocate" participate in at least some cases before the FISA Court.[99] Although the details vary, the basic gist is that Congress would create an independent office staffed by lawyers empowered to appear in at least some cases before the FISA Court, specifically tasked with arguing *against* the government's interpretation of the relevant statutory and constitutional authorities. Such lawyers would have security clearances—allowing the FISA Court to entertain such arguments in secret—and would not formally represent a "client."[100] Instead, their statutory obligation would be to play the devil's advocate—to assist the FISA Court by providing alternative possible readings of the same procedural, evidentiary, statutory, and

---

whereas cooperation is reimbursed. *See, e.g.*, *id.* § 1881a(h)(2) ("The Government shall compensate, at the prevailing rate, an electronic communication service provider for providing information, facilities, or assistance in accordance with a directive issued pursuant to paragraph (1).").

97. *See* Letter from Hon. Reggie B. Walton, Presiding Judge, FISC, to Hon. Patrick J. Leahy, Chairman, Sen. Comm. on the Judiciary, at 8–9 (July 29, 2013), *available at* http://www.leahy.senate.gov/download/honorable-patrick-j-leahy.

98. Indeed, the only public record of a wholly adversarial proceeding before the FISA Court came under the now-defunct Protect America Act of 2007, Pub. L. No. 110-55, § 2, 121 Stat. 552, 554–55 (formerly codified at 50 U.S.C. § 1805b), and culminated in the FISA Court of Review's 2008 decision in *In re Directives [Redacted] Pursuant to Section 105B of the Foreign Intelligence Surveillance Act*, 551 F.3d 1004 (FISA Ct. Rev. 2008). As we now know, Yahoo! was the adversarial party in that case.

99. *See, e.g.*, Carr, *supra* note 85.

100. It should follow that, if the "special advocate" *was* tasked with representing U.S. persons who are subject to FISA Court-approved surveillance, then the only Article III issue would be the post-*Clapper* standing question addressed in Part II, and the adverseness and appellate standing issues discussed herein would be moot.

constitutional language on which the government has rested its application.[101]

At least with regard to proceedings before the FISA Court, the creation of a "special advocate," however conceived, should not raise any new Article III concerns (if anything, it should mitigate any existing constitutional objections).[102] Assuming *arguendo* that these disputes *already* comport with Article III's justiciability requirements, it is difficult to see how adding a new party in suits initiated by the government as plaintiff would raise any new concerns. Although reasonable people will certainly disagree about the wisdom of competing "special advocate" proposals as a matter of policy, it is difficult to dispute their validity as a matter of law—at least in proceedings before the FISA Court.

## C. Standing to Appeal

Where things get tricky—and where Article III standing doctrine again rears its jurisprudential head—is if and when the special advocate *loses* before the FISA Court, and seeks to appeal an adverse decision to the FISA Court of Review. After all, parties must have Article III standing not just at the beginning of a suit (which exists in the FISA context thanks to the government's role), but also standing to *appeal*.[103] In the context of appellate standing, the Supreme Court has held that such standing *can* arise merely from an adverse decision below—but only so long as that decision caused a specific and concrete injury to the party seeking to appeal.[104]

Consider, for example, the Court's June 2013 decision in *Hollingsworth* v. *Perry*—the case challenging California's ban on gay

---

101. For two of the more comprehensive proposals in this regard, compare the FISA Accountability and Privacy Protection Act of 2013, S. 1215, 113th Cong. (2013), and the FISA Court Reform Act of 2013, S. 1467, 113th Cong. (2013). *See generally* Mark M. Jaycox, *EFF's Cheat Sheet to Congress' Spying Bills*, EFF.ORG, Sept. 11, 2013, https://www.eff.org/deeplinks/2013/08/effs-cheat-sheet.

102. *See* Marty Lederman & Steve Vladeck, *The Constitutionality of a FISA "Special Advocate,"* JUST SECURITY, Nov. 4, 2013 (1:34 p.m.), http://justsecurity.org/2013/11/04/fisa-special-advocate-constitution/.

103. *See, e.g.*, Arizonans for Official English v. Arizona, 520 U.S. 43, 64 (1997).

104. *See* ASARCO Inc. v. Kadish, 490 U.S. 605, 617 (1989); Diamond v. Charles, 476 U.S. 54, 62 (1986).

marriage, "Proposition 8."[105] In *Perry*, there was no question that the plaintiffs had standing in the district court to challenge Prop. 8 on federal constitutional grounds. But once the district court ruled in their favor, the state declined to appeal. Instead, a group of proponents and local government officials who had intervened in the district court sought to challenge the district court's decision on appeal.[106] Writing for a 5-4 majority (that did not include Justice Kennedy), Chief Justice Roberts held that the proponents lacked appellate standing:

> To have standing, a litigant must seek relief for an injury that affects him in a "personal and individual way." He must possess a "direct stake in the outcome" of the case. Here, however, petitioners had no "direct stake" in the outcome of their appeal. Their only interest in having the District Court order reversed was to vindicate the constitutional validity of a generally applicable California law.[107]

Rejecting the cases marshaled by Justice Kennedy's dissent, Chief Justice Roberts concluded by stressing that "none comes close to establishing that mere authorization to represent a third party's interests is sufficient to confer Article III standing on private parties with no injury of their own."[108] And although the intervenors might have been able to claim standing if they were acting as "agents" of the state, it was clear from the record that no such agency relationship existed.[109]

Dissenting, Justice Kennedy suggested that the Chief Justice's opinion was marked with "much irony."[110] After all, "A prime purpose of justiciability is to ensure vigorous advocacy, yet the Court insists upon litigation conducted by state officials whose preference is to lose the

105. 133 S. Ct. 2652 (2013).

106. After certifying a question of state law to the California Supreme Court, *see* Perry v. Schwarzenegger, 628 F.3d 1191 (9th Cir. 2011); Perry v. Brown, 265 P.3d 1002 (Cal. 2011), the Ninth Circuit held that the intervenors *did* have standing. *See* Perry v. Brown, 671 F.3d 1052 (9th Cir. 2012), *vacated*, 133 S. Ct. 2652.

107. 133 S. Ct. at 2652 (citations omitted).

108. *Id.* at 2665.

109. *See id.* at 2666–67.

110. *Id.* at 2674 (Kennedy, J., dissenting).

case."[111] Indeed, as Justice Kennedy explained, "The doctrine is meant to ensure that courts are responsible and constrained in their power, but the Court's opinion today means that a single district court can make a decision with far-reaching effects that cannot be reviewed."[112]

One could make similar arguments about appellate standing in the context of a FISA "special advocate." Given the unique and effectively non-adversarial nature of proceedings before the FISA Court, allowing a special advocate would help to "ensure vigorous advocacy"; authorizing an appeal from an adverse decision would protect against a scenario wherein "a single district court can make a decision with far-reaching effects that cannot be reviewed." Once again, then, if the question is simply whether Justice Kennedy would endorse standing on such terms, the case law provides a fairly clear answer. And yet, if *Perry* is taken at face value, it seems just as clear that there are five votes for the contrary proposition—and for no appellate standing for a party like the "special advocate" at the heart of many of the current FISA reform proposals, unless it incurs a specific and concrete injury as a direct result of an adverse decision by the FISA Court.[113]

### D. The Unanswered Question: Congress and Appellate Standing

To be sure, *Perry* raised the question of whether *states* could create an interest sufficient to confer appellate standing upon a party not directly injured by the decision below. Another possibility, and one not considered in *Perry*, is whether *Congress* could do so. As Justice Kennedy pointed out

---

111. *Id.*

112. *Id.*

113. Congress could also sidestep the constraints on appellate standing by providing for appeals *qua* judicial certification, as is currently the case under 28 U.S.C. § 1292(b) for interlocutory appeals, and § 1254(2) for questions certified to the U.S. Supreme Court. Although there is no authority addressing the extent to which Article III standing principles apply to judicially certified questions, there is also no suggestion that an appellate court would lack the power to answer certified questions from a lower court—especially where, as here, *that* court was possessed of a live and adversarial dispute. Congress might also borrow a page from the context of bankruptcy courts, where those courts are allowed to act finally with regard to "core" bankruptcy matters, but may only make recommendations (that must be confirmed by the district court) in "non-core" matters. *See* 28 U.S.C. § 157. Although the specifics of these approaches are beyond the scope of this essay, the larger point they underscore is the array of options potentially available to Congress beyond a direct statutory appeal *by* the special advocate.

in his dissent, the Supreme Court has previously recognized Article III standing for private parties to prosecute criminal contempt and *qui tam* actions (in both of which they are proceeding on behalf of the federal government); for "next friends" suing on behalf of the real party in interest; and for shareholders in shareholder-derivative suits.[114]

And at least in the contempt, *qui tam*, and shareholder-derivative contexts, those suits are pursuant to express statutory authorization—authorization that arguably does *not* create the agency relationship upon which the *Perry* majority appeared to base their distinction.[115] Thus, perhaps one way to reconcile these seemingly divergent decisions is by concluding that Congress has—and would have—greater latitude to confer appellate standing upon those not directly injured by a lower-court decision than states do after *Perry*, analogizing to the greater latitude Justice Kennedy would give (and has given) to Congress after and in light of *Lujan*.

* * *

In one sense, perhaps the most important takeaway from the above analysis is the extent to which the Supreme Court's Article III standing jurisprudence interposes substantial obstacles to judicial review of secret surveillance programs (if not all secret government conduct) on the merits. Yes, Justice Kennedy's *Lujan* concurrence appears to leave *more* room for Congress to authorize challenges to secret surveillance programs based on evidence that interception of the plaintiffs' communications is reasonably likely, if not "certainly impending." And yes, no Article III obstacle should prevent Congress from expanding the scope and volume of adversarial participation in matters before the FISA Court, even if Article III may present difficulties in allowing such statutory adversaries to appeal adverse decisions to the FISA Court of Review and, if necessary, the Supreme Court. Thus, those who seek reforms of the FISA process with an eye toward increased accountability and oversight could certainly look to these remedies as useful steps in that direction.

But if nothing else is clear, it should hopefully be obvious that a truly comprehensive scheme for adversarial judicial review of secret surveillance programs may in fact be unobtainable, at least without sacrificing the very secrecy that arguably enables the *success* of such

114. *Perry*, 133 S. Ct. at 2673–74 (Kennedy, J., dissenting).

115. *Id.* at 2666–67 (majority opinion).

governmental foreign intelligence activities.[116] That is to say, absent some meaningful shift in the Supreme Court's understanding of the constraints Article III's case-or-controversy requirement imposes upon the adjudicatory power of the federal courts, or far greater (if not mandatory) participation in the FISA process by those entities that *receive* production orders and intelligence directives under the statute, it may not in fact be constitutionally possible to provide in all or even most cases for meaningful adversarial review. This does not mean, of course, that Congress should not try to so provide to the maximum extent feasible; if anything, it only underscores the extent to which such review cannot be the sum total of efforts to "reform" the foreign intelligence surveillance activities of the U.S. government, at least for those who truly believe that such reform is warranted.

116. This point distinguishes the Guantánamo detainee cases, for example, or proceedings before the as-yet-unused Alien Terrorist Removal Court, *see* 8 U.S.C. § 1534(e)(3)(F), in both of which security cleared counsel *are* authorized to represent the subjects of the government's counterterrorism authorities. In those settings, the subjects are *aware* of the government's general policies; they are merely not privy to that evidence relevant to their case which is properly classified. *See* David Cole & Stephen I. Vladeck, *Comparative Advantages: Secret Evidence and "Cleared Counsel" in the United States, the United Kingdom, and Canada*, in SECRECY, NATIONAL SECURITY, AND THE VINDICATION OF CONSTITUTIONAL LAW 173 (David Cole et al., eds., 2013). In the surveillance context, in contrast, it would defeat the purpose if the subjects of the government's secret foreign intelligence surveillance activities were aware of their targeting in the first place.

Preliminary Draft – Please Do Not Cite Without Permission
To be Published in *I/S: A Journal of Law and Policy for the Information Society*
9 ISJLP ___ (2014).
http://www.is-journal.org

# Making No Secrets About It

**Reed E. Hundt**

When Big Government cajoles Big Companies to share Big Data, the question inescapably follows: What should be the governing rules for digital information?

Law, regulation and norms relating to the analog world – that which people see, hear, smell, touch, and taste – do not translate well to the digital world. Everything that can be known is being memorialized in the domain of electromagnetic signals that codify information in volume too vast and patterns too complex for humans to understand. The five senses have no presence in the digital world. Flesh and blood people can send messages – queries, instructions, information – into the digital network of circuits and electromagnetic waves. Responses come back: the restaurant expects you and your five senses at 8 p.m. and here are the directions to get there.

But behind the response, in the near infinitude of electrical circuits, no human can even pretend to keep up with the digital collection and use of information. All information can be recorded, and almost all soon will be, in the computers of the digital domain. By "information" must be meant any observation, transmission, calculation or memorialization. The information may relate to something at rest (the restaurant door recorded by a surveillance camera, the restaurant's seating chart and menu) or in motion (a tweet about the menu, a credit card payment

for dinner). It will include, in Peirce's taxonomy, evidence of "signs," assumptions about "objects," and the provision of "interpretants." [1]

The networked computers of the digital domains not only preserve the "signs," but they draw conclusions about the "objects" to which the signs relate: with that prix fixe meal, amuse-bouches are to be expected. They constantly seek and create patterns from which they draw conclusions ("interpretants") of at least two kinds: what caused an action to occur in the past and what is causing actions probably to occur in the future. People have gone to this restaurant because they know it serve paté off the menu and under the table; people will continue to go because San Francisco has banned paté. The computers know everything that can be known. They also opine and predict. They will keep their views to themselves or share them with humans, at least in simplified form.

The computers keep most of their data to themselves because the volume of digital data is too large for any person to review within the span of human life. The computers manage that data too quickly for any human to follow by hand or eye. Humans can understand the digital domain only in two ways: in theory and in the practical form of receiving answers to questions (yes, that particular San Francisco restaurant offers paté off the menu).

Some may draw the corollary that humans should be indifferent if machines turn every sign and symbol of an individual's "thoughts, sentiments, and emotions"[2] into computer code. No one needs to be concerned about computers knowing everything about everyone. Similarly, you should not worry if the shining sun sees you lounging naked in your back yard. If some are not much troubled by learning how much data lies in data banks, they may believe humans have a right of privacy only as against the intrusions of other humans.

[1] See http://www.helsinki.fi/science/commens/dictionary.html
[2] Warren & Brandeis, "The Right to Privacy," 4 Harvard Law Review No. 5, December 15, 1890.

The digital domain may well be as inaccessible and mysterious as the stars. It may operate under rules as seemingly irrelevant to our analog world as Einsteinian relativity. Yet when the nuclear reactors of Fukushima melt down, the most abstruse laws of physics have manifold impact on the world that humans do feel with their five senses. When the digital domain intersects with the analog, its vast power can completely alter the way we live. Humans, or at least those possessing state-granted authority, can command that point of intersection. They can and do decide when and how the digital will have impact on the analog, when and how the opinions and predictions of the digital domain will lead to inquisition or incarceration in the physical world. Because the digital does impact the analog, none of us should be unconcerned about what computers know about us. Only machines should be indifferent to machines.

I argue here that the doyens of the digital domain, comprising big businesses with big access to nearly infinite data and big government with nearly overwhelming persuasive power, are crafting the operational rules for governing digital information. Constraining the government's behavior is, as since the beginning of the United States, the Constitution. But the companies, courts, Congress and Executive Branch are reinterpreting our rights for the digital domain. However, secrecy, in both corporations and government, makes the rules difficult to discern.

Based on what little we humans (can) know, the emerging practices and constitutional interpretations applicable to the digital domain are likely to allow government to make more errors in preventing criminal acts or apprehending bad actors than will be acceptable to the sense of justice most of us hold. Under the developing practices for digital information, government will be allowed to use information to ends that most individuals would find unacceptable, even repugnant, potentially edging toward tyrannical. Further, the currently developing practices for

big government's use of big data will lead to staggering expenditures of taxpayer funds. That in turn will cause government to delegate its tasks to big data-collecting companies, turning them into satrapies of the central state. If allowed to flower, such corporatism would prove destructive of both economic and social freedom. Finally, I argue that government and private sector secrecy about the current rules enhances these three risks: error, misuse, and corporatism. If any or all of these trends develop, they will cause a deterioration of the trust relationship between any American and the government.[3] Without trust among individuals, firms and the state, even the most effective police force cannot assure a coherent, well-functioning society.

No one involved in the technological breakthroughs that raise these possibilities wants a part in creating such a dystopian future. Almost all want to preserve for Americans, if not the whole world, what playwright Tom Stoppard called "autonomous freedom, the freedom to think for oneself, to use one's discretion, . . .to apply common sense, and common humanity." [4] Therefore, for the purpose of such preservation, the new rules should be identified and debated. Better rules should be adopted than those being put in place. The Constitution should be applied to the digital domain, not *in hoc verba*, because those 18th century precepts do not translate clearly,[5] but in practical ways that continue to protect everyone who is relatively powerless as against those who are relatively powerful.

[3] To quote Richard Thaler: "Trust is really important in society, and anything we can do to increase trust is worthwhile. There's probably nothing you could do to help an economy grow faster than to increase the amount of trust in society." See http://www.minneapolisfed.org/publications_papers/pub_display.cfm?id=5184.
[4] "Tom Stoppard: Information is light," The Guardian, October 11, 2013.
[5] In an interview published October 6, 2013, Justice Scalia said as to originalism, "Words have meaning. And their meaning doesn't change." But technology can alter what words mean. When the Bill of Rights was adopted, purple meant to most people a color verging on red. Then in 1856 William Perkin invented a synthetic dye that made a more bluish color widely marketed and sold as "purple," the commercial success of which effectively shifted the meaning of the "purple" toward mauve. More recently, Facebook seems to have changed "friend" into a verb with evolving connotations.

What, then, are the current rules? At the appellate level, the large mobile carrier, Verizon, is now arguing that no law or regulation can govern access to the digital domain.[6] Verizon claims that the First Amendment does translate from analog to digital, and that it anoints Internet access as a kind of apostolic successor to the printing press. Because Verizon provides access to the Internet and the near infinitude of digital information therein, it is like a newspaper with a printing press that provides access to analog information. Hence, no government can make any law that constrains Verizon's behavior. Specifically, Verizon can decide who has access at what price (a newspaper can decide to whom it should sell and at what press). And Verizon can decide what to give access to (a newspaper can decide what to print). Verizon can choose, for example, what emails to send (a newspaper can decide what letters to the editor to print).

This argument mistakes conduit for content, according to the brief in that court filed on behalf of Susan Crawford, a well-known law professor, and me.[7] Verizon is a newspaper delivery truck, but not a newspaper or a printing press. Analogy, it seems, is the way that law maps the analog world of the drafters of the First Amendment to the digital domain. Analog values, like autonomous freedom, as well as analog objects like "printing presses," also must be restated in forms that make sense in the fusion of digital and analog experience that is the way we live now.

Without waiting for the Court of Appeals or Congress, Internet access providers (primarily telephone and cable companies) and over-the-top-of-Internet-access companies (Google, Facebook, Amazon, Yahoo, and others) are creating and following new rules to the

[6] Insert Verizon v fcc, pending case cite, d.c. circuit

[7] See http://scrawford.net/verizon-v-fcc-why-it-matters/.

digital domain. I'm going to call these firms "OTT," for "over the top." I will call the access providers "carriers."

The carriers keep track of the parties, geographic location and duration of all digital communication. They could ask the computers in their networks to examine and save the content of communications but as far as I know, they do not. Almost all digital communication goes over one or more of the networks owned by a mere handful of carriers. For many years, these carriers have shared with government what they know about digital communication, sometimes after receiving warrants, and sometimes without such formality.

The OTT firms transmit words, pictures, numbers (think: Gmail, Instagram, PayPal). They use the carriers' networks, but while transmitting the content they can and do have their computers review it. They save what they choose to save, which is a lot. They presumably believe, like the carriers, that the First Amendment bars government from interfering with their content practices. But as of this writing, no OTT firm has chosen to be the protagonist in a digital version of the *Pentagon Papers* case.[8] I suspect that none wants to reveal how it gathers information or how skimpy is the proof of consent from all of us who provide the information.

Besides, the OTT firms' case would not align them with the public interest. In *Pentagon Papers*, the newspaper championed the public's right to understand its government's actions against the government's attempt to keep its conduct secret. In opposing the government's efforts to get its hands on the OTT's firms' information about the public, the OTT firms would be arguing that their own largely secret data gathering is privileged over the government's secret actions. They would not be contending that they are the agents of individuals who use their services. If they invoked a right of privacy, it would be a business's right to keep it practices

[8] New York Times Co. v. United States, (per curiam) 403 U.S. 713, 91 S. Ct. 2140, 29 L. Ed. 2d 822 (1971)

secret from users, customers and competitors. Although such self-interest would not prejudice their claims in court, it would hardly inspire trust between the OTT firms and the users who provide the information which makes the firms successful.

For decades the government has been able to learn from carriers the location, parties and duration of telephone calls. It also has been able to wiretap lines and listen to conversations. Often government has obtained warrants in order to hear content; not always.[9] Because perhaps half or more than half of all global telephone communication went to, from, or through the United States, government in this country has also been able to eavesdrop on the bulk of global traffic. Other obliging countries presumably have filled in such gaps as existed. But in only the last few years has the government been able to collect and review the substance of almost every communication.[10] Here again, the global reach of American OTT firms has enabled the American government to take look at much of the world's digital content. Technological breakthroughs, more than executive or judicial action, have enabled these developments. Technology has preceded law. Law has been obedient to what is technologically possible; law has also been perplexed about technology, worried about taking any action that might enable another 9/11, and incapable of conceiving of a new paradigm for the digital domain.

In the United States, and worldwide, a small number of big firms have garnered huge market share in search, on-line media, digital payments, and other sorts of digital communications. The rise of Google and its ilk has enabled the American government to think big. If the American OTT firms had not been able to seduce from users all the information

[9] "In practice…an American's communication could be read without a warrant, another U.S. official says." "New Details Show Broader NSA Surveillance Reach," Wall Street Journal, August 20, 2013.
[10] "The system has the capacity to reach roughly 75% of all U.S. Internet traffic…" Ibid. See also "N.S.A. Gathers Data on Social Connections of U.S. Citizens," New York Times, September 28, 2013. ("The agency can augment the communications data with material from …commercial and other sources, including bank codes, insurance information, Facebook profiles, passenger manifests, … and GPS location information, as well as property records and unspecified tax data…")

imaginable, government could not have considered the uses it might make of this data.[11] Certainly government could never have gathered so much data about so many dimensions of human activity if the big companies had not obtained that from users. The rise of the big firms has also narrowed the group with which government has had to negotiate in order to get almost all information it can imagine it wants. Government can make offers these firms cannot refuse.

Nor could anyone in government have made much use of the data but for the technological breakthroughs in storage, retrieval, and calculation that commercial innovators have produced. A decade ago, microprocessors were neither fast enough nor cheap enough to store and analyze the volume of digital information generated in America, much less worldwide. Moore's Law, the prediction that microprocessing would double in performance or drop half in price every 18 months, has enabled government and the really big OTT firms to save and analyze even the vast quantities of digital information that Americans now create and consume. Computers now have programs that permit them to analyze data without first organizing it into columns and rows. Other programs permit computers to learn from their own mistakes. Still other software divides requests (do people really like the paté served under the table at that restaurant?) into discrete tasks to be performed by many different computers, as a result of which answers are delivered when they matter (yes, go ahead and order that paté right now!). [12] Progress in antennas, wireless transmission, drones, satellite camera, facial recognition,

[11] In many countries, government has long cemented the symbiotic relationship between telecommunications firms and government's desire to monitor communications by taking ownership stakes in the firms or by tightly regulating such firms. The OTT firms, however, have risen to become the chief data mongers in an era of privatization, in which the United States government, among others, has argued against mixing public and private capital in the same entity, on the grounds that such ownership distorts efficient market conduct. For this reason, government in the United States and philosophically aligned nations has been using tools other than ownership to obtain access to the data gathered by OTT firms.

[12] See "How the NSA Could Get So Smart So Fast," Wall Street Journal, June 12, 2013.

smartphones and many other technologies have extended further the scale and scope of digitizing and gathering information.

As a result of the new combination of big firms, big data and big government, government now routinely asks computers to suggest who has committed crimes. Government also asks computers to predict criminal activities at specific locations. And it requests computers to identify people who intend to commit crimes.[13] Presumably, government instructs the computers to generate lists of threats on a continuous basis, ranking them according to probabilities. The computers do machine learning; that is, they constantly refine their analytical skill. The humans in charge of the government's digital domain of course hope the predictions are accurate. But they cannot know for sure how reasonable are the computations,[14] and, short of wresting admissions from every identified suspect, they cannot validate every prediction.[15] Some of the criminals, in the past and predicted in future, are terrorists; that is, some hideous fervor drives them to kill civilians and destroy facilities integral to society. But we are not discussing here only terrorist activities. That category is too permeable and broad. The uses of the digital domain for analog police work are too plentiful for government to resist applying them to any and all criminal matters.

So this is the way the digital domain actually works. We assume. Little by little newspapers, still putting ink on paper for fingers to touch and eyes to see in the analog world, are

[13] See "Don't even think about it," The Economist, July 20, 2013.
[14] See "NSA: The Decision Problem," George Dyson, Edge, July 27, 2013 ("In modern computational terms…,there is no systematic way to determine, in advance, what every given string of code is going to do except to let the codes run, and find out.")
[15] If suspects are apprehended before they commit the act the computers say they intend – exactly what anti-terrorist efforts try to do – then the ultimate proof of accurate prediction, namely, the deed itself, is obviously never provided. See Dyson, ibid. ("The ultimate goal of signals intelligence and analysis is to learn not only what is being *said* , and what is being *done*, but what is being *thought.* ")

reporting the vastness of its reach. Little by little, individuals are grasping that the government is well on the way to becoming the panopticon.[16]

What does this tell us about the application of the Constitution to the digital domain? If we want to be grounded in the emerging reality of governmental conduct, at least some of the amendments we call our Bill of Rights should be read with the modifications stated below:

First Amendment: But the Government can learn where and how you worship, what you say, with whom you meet or communicate.

Second Amendment: But the Government can discover who has bought Arms and can keep track of those persons.

Third Amendment: But the Government can "quarter" virtually in any house, "without the consent of the Owner," technologies that permit the Government to learn any digitized activity by any person or by any device owned by any person.

Fourth Amendment: But the Government can search any device recording digital activity by any person, without obtaining a warrant or having any reason to believe any such person has committed or intends to commit any criminal act; Government can copy any record of any person's digital activity.

Fifth Amendment: But Government can place anyone under examination, as many times and as long as a computer declares such likelihood of having done, or possibly intending to do, a crime. Any person's digital information can be used against such person. Government can take and hold any person's digital information without any process of law specific to such person: a general mandate as to a class of persons or information suffices to justify any taking. No one has a property interest in any digital information at least as against government's possession of such

[16] Jeremy Bentham's late 18th century design of a building where a watchman could secretly observe the behavior of all occupants. See http://en.wikipedia.org/wiki/Panopticon.

information, no matter how obtained. At least until and unless the Supreme Court decides more cases involving digital information, the rights of individuals in the digital domain at least appear to be curtailed in these procrustean ways. The capabilities of big firms and big government currently are paramount as to digital data.

So what can go wrong? The answer depends on motive, competence, and constraints.

The carriers profit from transmitting the most information and seeking bottleneck pricing power over access. Saving and analyzing information is a cost they cannot recover, save in respect of learning better ways to send information. They do share freely with government, but they do not collect and store much content, at least as far as we know. Their motives to misuse digital data are limited; their competence is fairly high; they face constraining regulation at the FCC and in state regulatory authorities.

OTT firms, like the government, use digital data about past behavior in order to predict each person's future behavior. On the strength of that prediction – who might go to a particular restaurant, what might they order? – they sell placement to advertisers. The OTT firms will give anything away for free or nearly for free (operating systems, maps, news) in order to attract attention to the free material. Knowing the proclivities of those whose attention is thus captured on a screen the firms control, they sell to advertisers the opportunity to present, visibly, on the handheld or desktop screen, the specific goods and services they wish to sell to those whose previously gathered information suggests are likely to buy these categories of goods and services.

Supposedly it was 19$^{th}$ century merchant John Wanamaker who said, "Half the money I spend on advertising is wasted; the trouble is I don't know which half." Many of the OTT firms

aim to persuade modern day Wanamakers that in return for money they can reduce the waste by reporting exactly who saw the ad and then made the purchase.

Perhaps in the near future, OTT firms also will use the information they have gathered from all of us to provide answers to questions (what is the increase in my probable mortality before 70 if I eat that paté?) in return for money. But for now, the principal use is to provide advertisers solutions to the Wanamaker problem. OTT firms are hoisted on their own digital petard, however, because the digital domain also records patterns that seem to show the causal connection between advertising and purchase. As a result, OTT firms face the traditional constraint of capitalism. If they do not perform for their customers – give accurate predictions – then their customers can go elsewhere.

The government wants to use the same data for predictions. It is predicting not consumer purchases but criminal acts. However, the techniques of storing and analyzing the data are much the same for predicting both the benign and the malign acts of humans.

Now we come to the problem of error. The carriers' information (called "metadata") permits the government to assemble a narrative of a suspect's behavior. But its predictive capability is low. The OTT content is richer, more useful, but it neither is nor needs to be perfect in its forecasting. If OTT firms are 75% accurate, or even 65% accurate, in predicting possible purchases, they offer much better value to advertisers than other media. If the government's predictions of terrorist activity were as far off as that, however, they would be of little use. Moreover, when it comes to the conviction of perpetrators of crimes, government needs to be even more accurate. Did someone steal the paté? What does the camera in the kitchen show?

Government needs proof beyond a reasonable doubt. The computers managing the digital domain will struggle to give this level of accuracy.[17]

Even if percentage of accuracy in prediction is 95%, the false positive problem is huge. Assume a population of 300 million, and assume terrorists number 1,500. Assume further the computers identify all the terrorists. The problem is that the computers will include in the identification 5% of 300 million, or 15 million people. So of those, one out of every 10,000 will be a terrorist; for every terrorist, about 10,000 people will be misidentified as terrorists.[18] Given that these overbroad predictions are made every day, in short order millions of people in America would be identified as terrorists. Misuse of information is of course possible for both OTT firms and government. Anyone at an OTT firm might leak information to those who want to harm the reputations of those surveilled. An OTT firm might follow the bad idea of selling personal information – like a private investigator in the analog era taking photos of cheating spouses. But the market really will mete out quick and serious punishment to OTT firms that misuse information. Trust is the key to the relationship of individuals to OTT firms. Moreover, individuals can have recourse to civil action if and when an OTT firm causes harm in ways cognizable as slander or defamation.

Misuse of data by government is both potentially far more draconian and subject to almost no remedy. Misuse by the government means: (a) disclosure that causes reputation and/or career harm to the innocent, (c) threat of disclosure that in turn silences opposition, competing points of view, dissent, and so threatens democracy's successful functioning, or (c) false arrest

[17] Law avoids stating its time-honored verbal standard in mathematical terms, but perhaps 95% probability is "beyond a reasonable doubt." See http://lpr.oxfordjournals.org/content/5/3-4/267.full.pdf.
[18] See http://bayesianbiologist.com/2013/06/06/how-likely-is-the-nsa-prism-program-to-catch-a-terrorist/. See also "Ethics Aside, Is NSA's Spy Tool Efficient?", Wall Street Journal, June 14, 2013.

based on unjustified targeting.[19] These are not the effects of misuse that OTT firms are likely to cause. We can assume with good grounds that the overwhelming proportion of government actors with access to the nearly infinite data of OTT firms do not intend any such harm. But it is said that more than a million people have access to classified information.[20] As the Snowden case illustrates, all kinds of people appear to know a lot about what government, through its computers at any rate, knows. And we don't have to go back farther than the Nixon Presidency to get a history lesson on the potential for data to be used for political purposes that make a mockery of democracy.

In sum, OTT firms have reasonably benign motives for wanting to obtain, store and analyze digital records of everything knowable in the world. They do not need to be completely competent in their predictions and yet can still can add much value to the commerce. They face meaningful checks and constraints on their potential misuse of everyone's data. The harm OTT firms are likely to do even in dire circumstances can be addressed by civil action and marketplace reaction.

By contrast, government's motives may be of the highest nobility, but government includes within its walls so many people that some surely harbor ill intentions on occasion or are merely clumsy in handling private information.[21] Under current rules and practice, bad government intentions are not, in the digital domain, much constrained. Nor can government be expected to predict with truly refined accuracy the bad acts intended by terrorists, or any

[19] See "U.S. surveillance architecture includes collection of revealing Internet, phone metadata," Washington Post, June 15, 2013 ("[NSA data] can…expose medical conditions, political or religious affiliations, confidential business negotiations and extramarital affairs.")

[20] "How Could We Blow This One," New York Times, July 3, 2013. ("some 1.4 million people (including, until recently, Snowden) hold "top secret" clearances.")

[21] "Two gamechanging NSA stories you must read," Washington Post, August 16, 2013 (NSA broke privacy rules or overstepped legal authority thousands of time every year since 2008)

criminals, from computer processes alone. Finally, under the current actual practices in the digital domain, checks and constraints on government misuse of data are not commensurate with the sort of harm to innocents that government action can inflict.

Now let us turn to the next category of difficulty: expense. The more data gathered by winning OTT firms, the more profits they make. The more data gathered by government, the more costs go up. There are no incoming streams of revenue to be obtained by government. Of course, if government can forfend a terrorist attack by obtaining predictions from databases, the savings measured in lives and also impact on the economy may be incalculable. A budget problem remains: there is no way to link the benefits of stopping crime with the cost of preventing it.

The OTT firms can be left to strike their own compromises with how much data to gather and the cost of collecting, storing and analyzing it. Typically the lines are crossed with respect to storage. OTT firms do not much need old information. When the data is old and cold, they will throw it away. Government would like to hold all information forever, because sleeper cells and clandestine agents might spend years formulating their dread plots. But storage is not free.

Moreover, OTT firms tend to specialize. By contrast, in government, agencies compete on the basis of gathering similar information for similar purposes. It is possible that one person running one entity will emerge as the steward of all government data; certainly General Alexander of the National Security Agency would be the leading candidate as of now. But when he retires in 2014, or when a new President arrives in 2017, there is no telling what person or agency may become the leading data analyzer. This governmental competition can provide presidents with useful conflict in points of view and judgment. But it can lead to astonishingly expensive duplication in the digital domain.

In any event, the volume of data is growing too fast for almost any government, and perhaps even the extraordinary American government, to manage. It is said that 90% of all digital information was created in the last two years.[22] In the next two years, even a greater volume will swell the data centers of the world. Few if any countries can afford to keep up. Perhaps only America and China can manage the data desired for national security purposes. Then, the United States may offer allies a digital umbrella, under which any participating nation can get access to the predictive capabilities of the American security system. They will be expected to use their police forces appropriately to apprehend suspects. In a system not unlike, but far less dangerous, than the nuclear umbrella erected in the Cold War, the United States could become a global peacekeeper without nearly the number of boots on the ground, and casualties that have come from the interventions in Iraq and Afghanistan.

Nevertheless, not even the United States can afford to gather, store and analyze all digital data.[23] Private firms simply must cooperate with government. If America is to offer its digital security capabilities to allies, then OTT firms in those allied countries also must cooperate in collecting and managing data.

At present OTT firms are leery of being involved with government. Some have filed lawsuits against the United States government concerning access to their data banks. But government needs that access, and the firms need governmental protection against cybersecurity threats. Therefore, the compact between OTT firms and government must be renewed, under new rules. Those who are surveilled – the people who provide the data -- can seek a seat at the table in this negotiation.

---

[22] See http://emerging.uschamber.com/library/2013/05/big-data-and-what-it-means

[23] See http://www.ianwelsh.net/the-logic-of-the-surveillance-state/ ("The problem with surveillance states…is the cost…both direct, in the resources that are required, and indirect in the lost productivity and creativity…")

Now we move to the ultimate problem: secrecy. As the late Senator Pat Moynihan wrote in his brilliant book by that name, secrecy in government is a form of regulation.[24] It is a rule that alters other rules. Specifically, secrecy impairs the rule against misuse of data and exacerbates the problem of expense.

When the government's activities in the digital domain are secret, motives and competence are not subject to beneficial scrutiny. Bad actors in government are far less likely to be sussed out when few, even in government, know who knows what about whom. The problems of inaccurate predictions and false positives are not even likely to be admitted, when secrecy precludes the problems from being discussed. No one will try to fix these problems, if wrong predictions are as likely to be acted upon as right ones; yet under conditions of secrecy that will be the case.

You might say that the agency with the data will do the checking. But everyone needs a boss to force thorough reviews from time to time. With secrecy there aren't many bosses, if any. This is what various Senators have been saying for some time about the data gathering in the Executive Branch.

Secrecy also limits human judgment. If hardly anyone has sanctioned access to information, then hardly anyone can debate decisions in front of, say, the President. The one who reports what the computers have concluded is the one who holds the single trump card. It may be the Queen of Spades in a game of hearts, but secrecy does not permit anyone to know what is really on the card.

Secrecy also makes expenses go up in at least two ways. Agencies whose activities are largely secret from each other do not know how to share resources. And secrecy within

[24] D.P. Moynihan: Secrecy, page 59 (Yale 1998)

government also exacerbates competition among agencies. In the private sector, consumers benefit if Microsoft secretly develops a faster, better, cheaper version of an Apple product. But in government, taxpayers pay more, not less, when agencies try to outdo each other.

The ultimate bane of secrecy is that it inspires distrust between the governed and their government. Since the founding of the United States of America, the citizens of our country have had more reason to believe in the good intentions of their government than, say, Russians or the Chinese. But the United States was not founded on the assumption that citizens simply must trust their government. Indeed, the opposite.[25] The Constitution, especially as amended by the Bill of Rights, is very much about constraining government in order to make it trustworthy.

When Americans do not know what government knows about each person, or what it does with that knowledge, then distrust will surely be on the rise. Eventually, there is a tipping point. When enough people distrust the government on enough topics for long enough a time, there is no police power that can stop that same distrust from affecting all social and business relations in society. The country will fall apart. It has happened to other countries; it is not impossible for distrust to be the cancer that kills the American idea.

I think these are some, if perhaps not all, the reasons why the new rules that are emerging are not good enough for the long run of the digital era. They are not terrible first drafts. For example, it is probably best for private firms to gather digital information from each of us, rather than having government do it directly, as General Alexander seemed to suggest he would prefer. But they are only first drafts. Here's an outline for a next draft of the governing rules of the digital domain.

[25] See Shane:Madison's Nightmare (Chicago, 2009)

Because secrecy enhances both misuse and expense, let's start with that topic. Here's what should be open either to individuals or to society, as appropriate:

a. Any individual should be able to know everything that an OTT firm knows about that person. This may encourage some to opt out of OTT data collection efforts. But then security forces can focus limited resources of the class of opt-outs, which is more likely to include bad actors, actual or potential.

b. Any individual should be able to know whether government identified that person as a suspected criminal any time in past up to five years ago. If so identified, you should be able to go to a court to seek exoneration and receive a monetary payment for the intrusion on your privacy if there was no reasonable basis for the government conclusion. This should constrain government excess, reduce cost, and improve trust, at least a little. (This also will improve accuracy.)

c. Everyone in society should be able to know in the abstract that government is doing – not whose phone numbers and emails the government thinks are revealing a crime but the fact that there are categories of such information being gathered. This will improve trust and accuracy and permit a debate about appropriate expense.

d. Everyone in society should know clearly where digital data is gathered and who in government is using it. There should be one central data gathering agency. There must be clear accountability. Responsibility for good stewardship must lie in named people, not in "government" writ broadly and ambiguously. Those responsible for misuse of data must be held to account.

e. The public should have access to records of all Presidential knowledge of results of surveillance within five years of presidential term ending, or 10 if need be shown to a court to

keep secrets longer. This information will improve the quality of reports to the President and constrain the likelihood of inappropriate requests by the President or staff.

A bureau of declassification should constantly reduce the amount of information treated as secret. Hardly anyone should be allowed security clearances that permit access to conclusions from digital data. The second step is to institute safeguards against abuse.

a. Those who have access to conclusions from the government's digital data banks should have term limits. We do not need a digital era Hoover. Five-year terms suffice; it is particularly important to minimize the political power of the executives running the government's digital domain by increasing the likelihood that they will not serve much longer than a Presidential term.

b. We should expand the requirement for government to obtain warrants for obtaining certain information. The process of getting a warrant focuses the information gatherers.

c. The judiciary should have access to a standing technical oversight committee to review the methods and accuracy of government's digital domain. This sort of committee serves most expert agencies; judges should have the same sort of technical advice.

d. Individuals who have good grounds to believe they have been wronged by government misuse of data should be able to have a lawyer appointed for them to investigate what has occurred.

e. Defense lawyers should be able to examine the accuracy of what the government's digital domain concludes and predicts.

f. Government officials should face criminal sanctions for intentional misuse of data from the digital domain, and civil sanctions for unintended misuse.

g. Monetary awards should go to any individual who can prove that digital data about that person, regardless of how obtained, was misused by government or a private firm. Consequential damages should be allowed. No punitive damages or attorney's fees should be awarded.

The third step is to constrain the expense of managing the digital domain.

a. Government and the private sector should enter into an agreement of cooperation the terms of which are public.

b. The government should obtain continuous technical advice on efficient data storage and retrieval practices at use in the private sector. If government does not choose to adopt best commercial practices, it should explain in reasons to select Congressional committee.

c. The United States should propose the creation of a global anti-terrorism cyber task force. All participating nations should contribute to defray the expense.

The rules for the digital domain must enable government to try to uncover and prevent criminal activity of all sorts, especially including terrorism. At the same time the rules must promote trust between individuals on the one hand and data-gathering firms and government on the other. To achieve this balance, government should operate under rules that minimize secrecy, not security. We want less secrecy and greater security, not the opposite. Part of security is the protection of individuals against abuse, intentional or accidental, by data-gathering firms and government. Every person needs to know that in the digital domain, as well as in the analog world in which the Constitution was written, the government protects the less powerful from the more powerful.

The dystopian modification of the Bill of Rights outlined above need not necessarily emerge as the prevailing jurisprudence of the digital age. Many cases have yet to be decided. The

Supreme Court is still far from stitching together a coherent doctrine for the digital domain. However, it is high time for Congress to curtail the spread of secrecy in government culture. It is past time for Congress to establish safeguards against governmental abuse of digital data. Congress should not wait for the Judiciary before giving individuals the right to know what private firms and government knows about each person, and giving the public in general the right to know what sort of information in the abstract that the government is gathering. By these steps, Congress will assure that the Constitution continues to underpin our cherished ideals of freedom even if we find ourselves living, speaking, and being remembered in the digital domain.

Preliminary Draft – Please Do Not Cite Without Permission
To be Published in *I/S: A Journal of Law and Policy for the Information Society*
9 ISJLP ___ (2014).
http://www.is-journal.org

# A Cyber Age Privacy Doctrine: A Liberal Communitarian Approach[1]

Amitai Etzioni

A privacy doctrine built for the cyber age must address a radical change in the type and scale of violations that the nation—and the world—face, namely that the greatest threats to privacy come not at the point that personal information is collected, but rather from the secondary uses of such information. Often cited court cases, such as *Katz*, *Berger*, *Smith*, *Karo*, *Knotts*, *Kyllo*—and most recently *Jones*—concern whether or not the initial collection of information was legal. They do not address the fact that personal information that was legally obtained may nevertheless be used later to violate privacy. That the ways such information is stored, collated with other pieces of information, analyzed, and distributed or accessed—often entails very significant violations of privacy.[2] While a considerable number of laws and court cases cover these secondary usages of information, they do not come together to make a coherent doctrine of privacy—and most assuredly not one that addresses the unique challenges of the cyber age.[3]

---

[1] I am indebted to Ashley McKinless for extensive research assistance on this article, and to Alex Platt, Steven Bellovin, and Shaun Spencer for comments on a previous draft.

[2] Amitai Etzioni, *The Privacy Merchants: What Is To Be Done?*, 14 PENN. J. CONST. L. 929 (March 2012).

[3] Peter P. Swire, *Katz is Dead. Long Live Katz*, 102 MICH. L. REV. 904, 912 (2002) ("The increasing storage of telephone calls is part of the much broader expansion since 1967 of stored records in the hands of third parties. Although there are no Supreme Court cases on most of these categories of stored records, the Miller and Smith line

True, collected personal information was subject to secondary abuses even when it was largely paperbound (e.g., in police blotters or FBI files). Indeed, when Warren and Brandeis published their groundbreaking 1890 article in the Harvard Law Review, considered the "genesis of the right of privacy," they were not concerned about gossip per se (a first order privacy violation) but about the wider distribution of intimate details through the media (a secondary violation).[4] However, the digitization of information, the widespread use of the Internet and computers, and the introduction of artificial intelligence systems to analyze vast amounts of data have increased the extent, volume, scope, and kinds of secondary usages by so many orders of magnitude that it is difficult to find a proper expression to capture the import of this transformation.[5] The main point is not that information can now be processed at a tiny fraction of the cost and incomparably faster speeds than when it was paper bound, which is certainly the case, but that modes of analysis—which divine new personal information out of personal data previously collected—that are common today were simply inconceivable when most personal information was paper bound.[6] Because this observation is critical

---

of cases make it quite possible that the government can take all of these records without navigating Fourth Amendment protections.").

[4] Samuel D. Warren and Louis D. Brandeis, *The Right of Privacy*, 4 HARV. L. REV. 193 (1890).

[5] For an excellent overview of how advances in information and communication technologies have rendered obsolete the privacy laws (and the doctrines on which these laws are based) of the 1980s and 1990s, see Omer Tene, *Privacy: The new generations*, 1 INTERNATIONAL DATA PRIVACY LAW 15 (2011). For a discussion of how these changes have particularly affected the privacy expectations of the 'Facebook generation,' see Mary Graw Leary, *Reasonable Expectations of Privacy for Youth in a Digital Age*, 80 MISS. L. J. 1033 (2011).

[6] This is of course not a terribly new position—legal scholars have been discussing the implications for privacy and the Fourth Amendment of the Internet since its introduction as publically available technology. *See* LAWRENCE

to all that follows, and because the term "secondary usages" (which implies usages less important that the first or primary ones) is a rather weak one, I employ from here on the infelicitous term "cybernated information" (or cybernation) to refer to information that is digitized, stored, processed, and formatted for mass distribution. Cybernated data can be employed in two distinct ways and both represent a serious and growing threat to privacy. A discrete piece of personal information, collected a one point in time ("spot" information) may be used for some purpose other than what it was originally approved for, or spot information may be pieced together with other data to generate new information about the person's most inner and intimate life.

The cyber age privacy doctrine must lay down the foundations on which Congress can develop laws and the courts can accumulate cases that will determine not merely what information the government may legally collect—but what it might do with that data. According to some legal scholars, the D.C. Circuit's decision in *Maynard* and the concurring opinion by the Supreme Court's justices in *Jones* provide the building blocks for this new edifice, sometimes referred to as a mosaic theory of the Fourth Amendment, under which "individual actions of law enforcement that are not searches for Fourth Amendment purposes may become

---

LESSIG, CODE AND OTHER LAWS OF CYBERSPACE 222-23 (1999) and Laurence H. Tribe, The Constitution in Cyberspace, Keynote Address at the First Conference on Computers, Freedom, & Privacy (March 26, 1991) (transcript available at www.sjgames.com/SS/tribe.html).

searches when taken together en masse."[7] This observation is based Justice Alito's argument that the GPS tracking of a vehicle on a public highway constituted a search because of the length of time over which the monitoring took place (28 days). This opens the door to take into account the volume of information collected, and presumes that, while limited amounts collection may be permissible, large amounts could constitute a violation of privacy. *Jones*, however, still only deals with collection. Hence, most of the work of laying down the foundations for the protection of privacy from cybernated information remains to be carried out.

The article first suggests that we cannot rely on the privacy expectations of individuals or society—principles introduced in *Katz*—in developing a new privacy doctrine for the cyber age (Part I, a). The article then briefly indicates that a return to the home as the major focus of privacy will not serve either, and we are to consider privacy as a protective sphere that follows the individual regardless of place (Part I, b). The article then introduces a "social policy model" of the Fourth Amendment to move us forward.[8] Within this model, we shall see that defining what is minimally intrusive becomes a key issue; instead of treating intrusiveness

---

[7] Erin Smith Dennis, *A Mosaic Shield: Maynard, the Fourth Amendment, and Privacy Rights in the Digital Age*, 33 CARDOZO L. REV. 737 (2012). *See also* Orin Kerr, *The Mosaic Theory of the Fourth Amendment,* 111 MICH. L. REV. 311, 320 (2012) ("Under mosaic theory, searches can be defined collectively as a sequence of discrete steps rather than as individualized steps. Identifying Fourth Amendment search requires analyzing police actions over time as a collective 'mosaic' of surveillance."); Madelaine Virgina Ford, *Mosaic Theory and the Fourth Amendment: How Jones Can Save Privacy in the Face of Evolving Technology*, 19 AM. U. J. GENDER SOC. POL'Y & L. 1351 (2011); Bethany L. Dickman, *Untying Knotts: The Application of Mosaic Theory to GPS Surveillance in United States v. Maryland* 60 AM. U. L. REV. 731 (2011).

[8] Orin S. Kerr, *Four Models of Fourth Amendment Protection*, 60 STAN. L. REV. 503, 519 (2007).

as a discreet variable, however, we find it must be treated as a continuous one. That is, the intrusiveness of an act may be considered higher or lower, rather than either minimal or not (Part I, c).

Once it has cleared the way through these deliberations, the article will outline the three dimensions of a cyber age privacy cube: volume, sensitivity, and cybernation (Part II). The last section of paper deals with the issue of defining when the collection and cybernation of information along these dimensions violates privacy (Section III).

## Part I. Assumptions

a. Moving Beyond *Katz*

Since 1967, the U.S. legal system has drawn on the twin concepts of personal and societal expectations of privacy to determine whether a Fourth Amendment 'search' has taken place. This article assumes that relying on the expectation of privacy (personal and societal), as articulated by Justin Harlan in his concurring opinion in *Katz*, is indefensible and that it should be allowed to fade from legal practice. Indeed, Justice Harlan himself adopted rather quickly a critical view of his two-pronged test. Four years after *Katz*, in his dissent for *U.S. v. White*, Harlan wrote that "While these formulations represent an advance over the unsophisticated trespass analysis of the common law, they too have their

limitations and can, ultimately, lead to the substitution of words for analysis. The analysis must, in my view, transcend the search for subjective expectations."[9]

The reasonable expectation of privacy standard has since faced a range of strong criticism.[10] In his widely-cited article on the Fourth Amendment, Anthony G. Amsterdam writes,

> "An actual, subjective expectation of privacy obviously has no place in a statement of what Katz held or in a theory of what the fourth amendment protects. It can neither add to, nor can its absence detract from, an individual's claim to fourth amendment protection. If it could, the government could diminish each person's subjective expectations of privacy merely by announcing half-hourly on television that 1984 was being advanced by a decade and that we were all forthwith being placed under comprehensive electronic surveillance…Fortunately, neither Katz nor the fourth amendment asks what we expect of government. They tell us what we should demand of government."[11]

One leading scholar of the Fourth Amendment and privacy, Orin Kerr, concedes "What counts as a 'reasonable expectation of privacy' is very much up for grabs,"[12] while Charles Whitebread and Christopher Slobogin charge that the Supreme Court has sent "mixed signals" on how to apply this standard.[13]

---

[9] U.S. v. White, 401 U.S. 745 (1971)

[10] Shaun B. Spencer, *Reasonable Expectations and the Erosion of Privacy*, 39 SAN DIEGO L. REV. 843 (2002); Jim Harper, *Reforming the Fourth Amendment Privacy Doctrine*, 57 AM. U. L. REV. 5 (2008); Haley Plourde-Cole, *Back to Katz: Reasonable Expectation of Privacy in the Facebook Age,* FORDHAM URB. L. J. (2010); Christopher Slobogin & Joseph E. Schumacher, *Reasonable Expectations of Privacy and Autonomy in Fourth Amendment Cases: An Empirical Look at Understandings Recognized and Permitted by Society*, 42 DUKE L.J. 727 (1993); Richard G. Wilkins, *Defining The 'Reasonable Expectation Of Privacy': An Emerging Tripartite Analysis*, 40 Vand. L. Rev. 1077, 1108 (1987); Sherry F. Colb, *What Is A Search? Two Conceptual Flaws In Fourth Amendment Doctrine And Some Hints Of A Remedy*, 55 Stan. L. Rev. 119, 122 (2002); Silas Wasserstom & Louis Michael Seidman, *The Fourth Amendment as Constitutional Theory*, 77 Geo. L.J. 19 (1988).

[11] Anthony G. Amsterdam, Perspectives on the Fourth Amendment, 58 MINN. L. REV. 349, 383 (1974).

[12] Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801, 808 (2004).

[13] Charles H. Whitebread & Christopher Slobogin, Criminal Procedure: An Analysis of Cases and Concepts,

The absurdity of *Katz* is revealed by contemplating the following example: Assume a municipal government announces that, for public health reasons, anyone who relieves themselves in a public pool would be charged with a misdemeanor. This government would then insert a dye (which unfortunately only exists in Hollywood's fertile imagination) that would form a dark blue cloud around anyone who violates the ordinance, but would not announce the introduction of this dye. By *Katz*, surely a person could argue that his expectation of privacy has been grossly violated, as he did not expect to be detected peeing in the pool. Would it be reasonable, therefore, to dismiss the charges against him and to rule the ordinance unconstitutional? And once the introduction of the dye is made public—how many people would have to know about it before it is no longer reasonable to expect privacy in the matter? And as determined by whom and how? Would one announcement about the new dye suffice, or must it be regularly advertised?

Or, take those who speak in a sizeable political meeting. They may well have no expectation of privacy. However, surely they should be protected from government surveillance in such a setting under most circumstances, to protect their privacy (among other reasons).[14] And do new technologies change what is

---

§ 4.03(f) at 116 (3d ed.1993).

[14] Further, what is considered a reasonable expectation is in constant flux due to technological changes. Thus, as the use of the Internet for personal communications grew, the Electronic Communications Privacy Act of 1986 failed protect stored private emails because it was passed in a time when most emails were related to business records, which are expected to be afforded a lesser degree of privacy. *See* Deirdre L. Mulligan Deirdre L. Mulligan, *Reasonable Expectations in Electronic Communications: A Critical Perspective on the Electronic Communications Privacy Act*, 72 GEO. WASH. L. REV. 1557 (2004).

expected, with, say, Facebook lowering the standards of privacy because so many people post so much private information? ECPA only protects emails for 90 days, during which time a warrant is needed for the government to read them. After that, a subpoena from any prosecutor will do, without judicial oversight, because in 1986 the thought of keeping emails around that long was ridiculous because the cost of storing them was so high.

As to the societal expectation of privacy, a sociologist is keen to know which, if any, communities will be polled to establish what this expectation is. The community of which the defendant is a member? Say Spanish Harlem? Or the city of New York? The American community? Or—the judge's country club? The fact that judges are free to assume they can rely on their sociological instincts as to what the community expects seems a strange foundation to rely on to determine when a search violates the Constitution.[15]

Finally, sociologists would be quick to agree that the whole notion is circular. Mr. Katz—and all others—either has or does not have an expectation of privacy *depending on what the court rules*. Jim Harper put it well when he wrote:

[15] ROBERT M. BLOOM, SEARCHES, SEIZURES, AND WARRANTS 46 (2003) ("Because there is no straightforward answer to this question, 'reasonable' has largely come to mean what a majority of the Supreme Court Justices say is reasonable.")

"Societal expectations are guided by judicial rulings, which are supposedly guided by societal expectations, which in turn are guided by judicial rulings, and so on."[16]

Four years after the Supreme Court ruled that the police had violated Katz's Fourth Amendment rights by bugging a public pay phone without a warrant, the Court held in *United States v. White* that no warrant was needed to record a conversation in a private home![17] A sociologist would expect that Mr. White has a higher expectation of privacy in his home than Mr. Katz has in a public phone booth. Nor is there any reason to believe that 'society' found the government's surveillance to be more reasonable in White's home.

Particularly relevant to what follows is that various court cases that draw on *Katz* seem not to recognize a 'split condition'—that is, situations in which the government collects information in a way that would be considered legal because it was "expected," but then uses and distributes it in "unexpected" ways, which would, thus, be illegal. There are, of course, many such split situations, and these situations should be covered by any comprehensive theory of privacy.

In short, it is difficult for a reasonable person to make sense out of *Katz*. Court rulings on whether a collection of personal information is a 'search' by

---

[16] Jim Harper, Reforming Fourth Amendment Privacy Doctrines, 57 AM. U. L. REV.138. *See also* JEFFREY ROSEN, THE UNWANTED GAZE: THE DESTRUCTION OF PRIVACY IN AMERICA 60 (2001) ("Harlan's test was applauded as a victory for privacy, but it soon became clear that it was entirely circular."); Michael Abramowics, *Constitutional Cicularity*, 49 UCLA L. REV. 1, 60-61 ("Fourth Amendment doctrine, moreover, is circular, for someone can have a reasonable expectation of privacy in an area if and only if the Court has held that a search in that area would be unreasonable.").

[17] Cloud, *Symposium: Rube Goldberg Meets the Constitution: The Supreme Court, Technology and the Fourth Amendmen*t.

Justice Harlan's formula seem to be highly dependent on what judges divine a person or 'society' would expect, without determining in any half objective way what these expectations actually are. And—at the same time—such standards ignore that rulings on privacy recast these expectations.

b. <u>But Not Back to 'The Castle'</u>

While the time has come to leave behind the reasonable expectation standard, this is not to say that the courts should revert to pre-*Katz* Fourth Amendment analysis, which gave considerable weight to the home as the locus of privacy. In *Katz* the majority ruled that "the Fourth Amendment protects people, not places," rejecting the 'trespass' doctrine enunciated in *Olmstead.* However, even after this, the home remained largely inviolable in the eyes of the courts. It seems *Katz* did not detach Fourth Amendment safeguards from the home but rather extended the sphere of privacy beyond it to other protected spaces. Information collected about events in one's home is still often considered *a priori* a violation of privacy, while much more license is granted to the state in collecting information about conduct in public and commercial spaces. As Justice Scalia put it, "'At the very core' of the Fourth Amendment 'stands the right of a man to retreat into his own home and there be free from unreasonable governmental intrusion.' With few exceptions, the question whether a warrantless search of a home is reasonable and

hence constitutional must be answered no."[18] This is an idea that has deep roots in American and English common law: "zealous and frequent repetition of the adage that a 'man's house is his castle,' made it abundantly clear that both in England and the Colonies 'the freedom of one's house' was one of the most vital elements of English liberty."[19] In *Dow Chemical Company v. United States*, the court established the expectation of privacy was lower in an industrial plant than a home, because the latter "is fundamentally a sanctuary, where personal concepts of self and family are forged, where relationships are nurtured and where people normally feel free to express themselves in intimate ways."[20]

The inviolability of the home and the private/public distinction in privacy law has been roundly criticized by feminist scholars. Catharine MacKinnon writes the problem with granting the home extra protection is that "while the private has been a refuge for some, it has been a hellhole for others, often at the same time."[21] Linda McClain points out that freedom from state interference in the home "renders men unaccountable for what is done in private-rape, battery, and other exploitation."[22]

---

[18] Kyllo v. United States, 533 U.S. 27 (2001).
[19] Payton v. New York, 445 U.S. 573, 591–98 (1980).
[20] Dow. Chem. Co. v. United States, 749 F.2d 307, 314 (6th Cir. 1984), *aff'd*, 476 U.S. 227 (1986).
[21] Catharine A. MacKinnon, *Reflections on Sex Equality Under Law*, 100 YALE L. J. 1281, 1311 (1991).
[22] Linda C. McClain, *Inviolability and Privacy: The Castle, the Sanctuary, and the Body*, 7 YALE J.L. & HUMAN. 195, 209 (1995).

This article assumes that the private/public distinction is rapidly declining in importance in general[23] and with regard to privacy in particular.[24] Marc Jonathon Blitz made the case compelling with regard to the cyber age and hence is quoted here at some length:

> "The 1969 case Stanley v. Georgia forbade the government from restricting the books that an individual may read or the films he may watch "in the privacy of his own home." Since that time, the Supreme Court has repeatedly emphasized that Stanley's protection applies solely within the physical boundaries of the home: While obscene books or films are protected inside of the home, they are not protected en route to it—whether in a package sent by mail, in a suitcase one is carrying to one's house, or in a stream of data obtained through the Internet.
>
> However adequate this narrow reading of Stanley may have been in the four decades since the case was decided, it is ill-suited to the twenty-first century, where the in-home cultural life protected by the Court in Stanley inevitably spills over into, or connects with, electronic realms beyond it. Individuals increasingly watch films not, as the defendant in Stanley did, by bringing an eight millimeter film or other physical copy of the film into their house, but by streaming it through the Internet. Especially as eReaders, such as the Kindle, and tablets, such as the iPad, proliferate, individuals read books by downloading digital copies of them. They store their own artistic and written work not in a desk drawer or in a safe, but in the "cloud" of data storage offered to them on far-away servers."

Privacy, it follows, is hence best viewed as a personal sphere that follows an individual irrespective of location. This is a version of what Christopher Slobogin refers as the protection-of-personhood theory of privacy, which "views the right to

---

[23] Amitai Etzioni, *The Bankruptcy of Liberalism and Conservatism*, 128 PSQ 39 (2013).

[24] Christopher Slobogin, *Public Privacy: Camera Surveillance of Public Places And The Right to Anonymity*, 72 MISS. L. J. 213 (2002). Scott E. Sundby, *Everyman's Fourth Amendment: Privacy or Mutual Trust between Government and Citizen?*, 94 Columbia Law Review 1751, 1758–9(Oct., 1994), Bethany L. Dickman, *Untying Knotts: The Application of Mosaic Theory to GPS Surveillance in United States v. Maryland* 60 AM. U. L. REV. 731 (2011).

privacy as a means of ensuring individuals are free to define themselves."[25] Privacy plays the same role whether one is in the home or out in public: "because a substantial part of our personality is developed in public venues, through rituals of our daily lives that occur outside the home and outside the family, cameras that stultify public conduct can stifle personality development."[26] If the government uses a long distance 'shotgun mic' to eavesdrop on conversations of two persons walking in a public park, such a search is clearly more intrusive than if the government measured the heat setting in their kitchen. This is the case because conversations are much more revealing about the person, including their medical condition, political views and so on than is their preferred heat setting. (I turn below to the question whether information that reveals that one is committing a crime deserves extra protection.) In short, privacy is best not home bound.

c. A 'social policy' model of the Fourth Amendment

One way to proceed is to follow a version of what Orin Kerr calls "the policy model."[27] This is an instrumentalist approach that relies on normative judgments: "Judges must consider the consequences of regulating a particular type of government activity, weigh privacy and security interests, and opt for

[25] Christopher Slobogin, *Public Privacy: Camera Surveillance of Public Places And The Right to Anonymity*, 72 MISS. L. J. 213, 256 (2002)
[26] *Id.* at 257.
[27] *Id.* at 519.

the better rule."[28] The article next outlines the social, philosophical, and normative assumptions for such a model.

(i) In seeking to base a privacy doctrine not on the usual foundations of expectations or location, this article draws on a liberal communitarian philosophy that assumes that individual rights, such as the right to privacy, must be balanced with concerns for the common good, such as public health and national security.[29] In contrast, authoritarian and East Asian communitarians tend be exclusively concerned with the common good or pay mind to rights only to the extent that they serve the rulers' aims.[30] And at the opposite end of the spectrum, libertarians and several contemporary liberals privilege individual rights and autonomy over societal formulations of the common good. (Although the term 'common good' is not one often found in legal literature, its referent is rather close to what is meant by 'public interest,' which courts frequently recognize, with a similar concept found in the U.S. Constitution's reference to the quest for a "more perfect union.")

The Fourth Amendment reads, "The right of the people to be secure in their persons, houses, papers, and effects, against *unreasonable* searches and seizures, shall not be violated." This is a prime example of a liberal communitarian text because it does not employ the absolute, rights-focused language of many

[28] *Id.*

amendments (i.e., "Congress shall make *no* law"), but recognizes on the face of it that there are reasonable searches, understood as those in which a compelling public interest takes precedence over personal privacy.

(ii) This article assumes that the communitarian balance is meta-stable. That is, for societies to maintain a sound communitarian regime—a careful balance between individual rights and the common good—societies must constantly adjust their public policies and laws in response to changing external circumstances (e.g., 9/11) and internal developments (e.g., FBI overreach). Moreover, given that societal steering mechanisms are rather loose, societies tend to over steer and must correct their corrections with still further adjustments. For example, in the mid-1970s the Church and Pike Committees investigated abuses by the CIA, FBI and NSA, uncovering "domestic spying on Americans, harassment and disruption of targeted individuals and groups, assassination plots targeting foreign leaders, infiltration and manipulation of media and business."[31] As a result, Congress passed the Foreign Intelligence Surveillance Act of 1978 (FISA) and created the Foreign Intelligence Surveillance Court to limit the surveillance of American citizens by the U.S. government.[32] After 9/11, several reports concluded that the reforms had gone too far by blocking the type of interagency intelligence sharing

that could have forestalled the terrorist attacks.[33] As a result, the Patriot Act was enacted in a great rush and, according to its critics, sacrificed privacy excessively in order to enhance security and "correct" what are considered the excesses of the reforms the Church and Pike committees set into motion. Since then, the Patriot Act itself has been recalibrated.[34]

At each point in time, one must hence ask whether the society is tilting too far in one direction or the other. Civil libertarians tend to hold that rights in general and privacy in particular are not adequately protected. The government tends to hold that national security and public safety require additional limitations on privacy. It is the mission of legal scholars, public intellectuals, and concerned citizens to nurture normative dialogues that help sort out in which direction corrections must next be made.[35] (Note that often some tightening in one area ought to be combined with some easing in others. For instance, currently a case can be made that TSA screening regulations are too tight, while the monitoring of

---

[34] For a critical analysis of the "Information Sharing Paradigm" that has arisen in law enforcement and intelligence community since 9/11, *see* Peter P. Swire, *Privacy and Information Sharing in the War on Terrorism*, 51 VIL. L. REV. 260 (2006).

[35] Alexander Aleinikoff, writing in 1987, argued that the courts had entered the "age of balancing." "Balancing has been a vehicle primarily for weakening earlier categorical doctrines restricting governmental power to search and seize." T. Alexander Aleinikoff, *Constitutional Law in the Age of Balancing*, 96 YALE L. J. 943, 965 (1987). Many civil libertarians have argued that post-9/11, Fourth Amendment rights are being systematically eroded in the name of national security. *See* Jay Stanley, *Reviving the Fourth Amendment and American Privacy*, ACLU, May 28, 2010, http://www.aclu.org/blog/national-security-technology-and-liberty/reviving-fourth-amendment-and-american-privacy. *See also* Orin S. Kerr, *An Equilibrium-Adjustment Theory of the Fourth Amendment*, 125 HARV. L. REV. 476, 478 (2011) ("The theory of equilibrium-adjustment posits that the Supreme Court adjusts the scope of Fourth Amendment protection in response to new facts in order to restore the status quo level of protection. When changing technology or social practice expands government power, the Supreme Court tightens Fourth Amendment protection; when it threatens government power, the Supreme Court loosens constitutional protection.).

whether visitors and temporary residents committed to leave the U.S. actually did so is too loose).

Orin Kerr and Peter Swire engage in an important dialogue on whether the issues present above are best suited for treatment by the courts or by Congress, and whether they are largely viewed through the prism of the Fourth Amendment or Congressional acts. The following discussion treats both as if they were an amalgam.

(iii) Four criteria help specify the liberal communitarian approach to privacy.[36] First, a liberal democratic government will limit privacy only if it faces a well-documented and large scale threat to the common good (such as public safety or public health), not merely a hypothetical or one limited to few individuals or localities. (I avoid the term "clear and present danger," despite the similarity in meaning, because it has a specific legal reference, not here intended.) The main reason this threshold must be cleared is because modifying legal precepts—and with them the ethical, social, public philosophies that underlie them—endangers their legitimacy. Changes, therefore, should not be undertaken unless there is strong evidence that either the common good or privacy have been significantly undermined.

[36] *See* Amitai Etzioni, *The Limits of Privacy* (1999).

Secondly, if the finding is that the common good needs shoring up, one best seek to establish whether this goal can be achieved without introducing new limits on privacy. For instance, this is achieved when one removes personally identifying information (such as names, addresses and social security numbers) when medical records are needed by researchers, thus allowing access to data previously not accessible, e.g., of Medicare databanks. Various technical difficulties arise in securing the anonymity of the data. Several ingenious suggestions have been made to cope with this challenge.[37] Conversely, if privacy needs shoring up, one should look for ways to proceed that impose no "losses" to the common good. For instance, introducing audit trails.

Thirdly, to the extent that privacy-curbing measures must be introduced, they should be as little intrusive as possible. For example, many agree that drug tests should be conducted on those directly responsible for the lives of others, such as school bus drivers. Some employers, however, resort to highly intrusive visual surveillance to ensure that the sample is taken from the person who delivers it. Instead, one can rely on the much less intrusive procedure of measuring the temperature of the sample immediately upon delivery.

[37] See Note 78 below.

Fourthly, measures that ameliorate undesirable side effects of necessary privacy-diminishing measures are to be preferred over those that ignore these effects. Thus, if contact tracing is deemed necessary in order to fight the spread of infectious diseases to protect public health, efforts must be made to protect the anonymity of those involved. A third party may inform those who were in contact with an affected individual about such exposure and the therapeutic and protective measures they ought to next undertake, without disclosing the identity of the diagnosed person.

The application of these four balancing criteria helps to determine which correctives to a society's course are both needed and not excessive. This article focuses on the third criteria and seeks to address the question: what is least intrusive?

## Part II. Privacy as a three dimensional cube

In this section I attempt to show that in order to maintain privacy in the cyber age, boundaries on information that may be used by the government should be considered along three major dimensions: The level of sensitivity of the information, the volume of information collected, and the extent of cybernation (defined as digitization, processing, and distribution). These considerations guide

one to find the lowest level of intrusiveness holding constant the level of common good. (A society ought to tolerate more intrusiveness if there are valid reasons to hold that the threat to the public has significantly increased, e.g., there is an outbreak of a pandemic—and reassert a lower level of intrusiveness when such a threat has subsided.)

a. Sensitivity

One dimension is the level of sensitivity of the information. For instance, data about the person's medical condition is considered highly sensitive, as are one's political beliefs and conduct (e.g., voting) and personal thoughts. Financial information is ranked as less sensitive than medical information, while publically presented information (e.g., license plates) and routine consumer choices much less so.

These rankings are not based on "expectations of privacy" or on what this or that judge divines as societal expectations, but on acts of Congress.[38] Rather, they reflect shared social values and are the product of politics in the good sense of the term, of liberal democratic processes, and moral dialogues.[39] (Different nations may rank differently what they consider sensitive. For example, France strongly

[38] Shaun Spencer raises concerns around legislating privacy protections. *See* Shaun Spencer, *Reasonable Expectatoins and the Erosion of Privacy*, 39 SAN DIEGO L. REV. 843, 860 (2002) ("Given the powerful influence of various lobbies opposed to strong privacy protection, that role may best be described as a sine qua non. That is, unless the public has a strong desire for privacy in a particular area, attempts to pass legislation establishing that area as a private sphere are doomed to fail…To the extent that legislatures base privacy legislation on social values and norms, they necessarily rely on the same changing expectations as the judicial conception of privacy.")

[39] AMITAI ETZIONI, FROM EMPIRE TO COMMUNITY: A NEW APPROACH TO INTERNATIONAL RELATIONS 67–71(2004).

restricts the collection of information by the government about race, ethnicity, and religion although it rationale is not the protection of privacy but rather a strong assimilationist policy and separation of state and church.) For those who analyze the law in terms of the law and economics paradigm, disclosure of sensitive data causes more harm to the person by objective standards than data that are not sensitive. Thus, disclosure of one's medical condition may lead one to lose one's job or not be hired, be unable obtain a loan, or incur higher insurance costs, among other harms. In contrast, disclosure of the kinds of bread, cheese, or sheets one buys—may affect mainly the kind and amount of spam they receive.

A re-examination of *Kyllo* helps highlight this principle. If one goes by *Katz*, the legality of a thermal imaging search from outside the home depends on what one presumes personal and societal expectations to be. At least, in middle class American suburbs, people may consider such a heat reading a violation of their expectations. If one clings to the idea that 'my home is my castle,' measuring the heat inside the home is indeed a major violation of privacy. However, if one goes by the cyber age privacy doctrine here outlined such readings ranks very low on sensitivity—because they reveal nothing about the resident's medical, financial, or political preferences, let alone their thoughts. In effect, they detect an extremely low bandwidth of information. The information revealed is less consequential than what kind of cereal the person purchased or which brand of coffee

One may argue that the information about the level of heating is actually particularly sensitive because it reveals that a crime is being committed. Preventing crime is obviously a contribution to the common good. And given that in 2011 fewer than half of violent crimes and 20% of property crimes in the U.S. were resolved, some may well hold that public authorities are not excessively indulged when dealing with crime.[40] As to harm to the individuals involved, they would be harmed only if they had a right to commit a crime. As to the presumption of innocence, there is the public safety exception. The arguments against the notion that crime committed in a home (e.g., spousal abuse) deserves more protection than one committed in public, were already presented above. What is new here is that historically, when the Constitution was written, searching a home required a person to enter or peep, which would entail a high level of intrusiveness because the intruder could not but note other potentially sensitive information besides whether or not a crime was being committed. However, technologies that have a very narrow and crime-specific bandwidth (e.g., dogs that sniff for bombs or sensors that measure abnormal levels of heat) and are, hence, very lowly-intrusive, should be allowed. One may disagree with this line of analysis, but still accept that basic point that the less-intrusive collection of insensitive information should be tolerated, while collection of highly-sensitive information should be banned

[40] "Offenses Cleared," Uniform Crime Report: Crime in the United States 2011, Federal Bureau of Investigation (October 2012).

Many court cases treat the voluntary release of information to others (and by them to still others, discussed below under the third party doctrine) as if they all had the same level of sensitivity,[41] including phone numbers dialed,[42] copies of written checks,[43] documents given to an accountant,[44] newspaper records,[45] and even papers held by a defendant's attorney.[46] A privacy doctrine that follows the principles here outlined would grant persons more say about the secondary usages of sensitive information, while recognizing that the less sensitive information may be used and passed on without the individual's explicit consent.

Over the years, Congress has pieced together privacy law by addressing the protection of one kind of sensitive information at a time, rather than treating them in a comprehensive fashion. Thus, in 1973, the Department of Health, Education and Welfare developed the Code of Fair Information Practices to govern the collection and use of information by the federal government. The principles of the code were incorporated in the Privacy Act of 1974, which "prohibits unauthorized disclosures of the records [the federal government] protects. It also gives individuals the right to review records about themselves, to find out if these records have been disclosed, and to request corrections or amendments of these

[41] The following examples are laid out in Swire, *Katz is Dead. Long Live Katz,* 908 –9.
[42] Smith v. Maryland, 442 U.S. 735, 745 (1979).
[43] United States v. Miller, 425 U.S. 435 (1976).
[44] Couch v. United States, 409 U.S. 322 (1973).
[45] Zurcher v. Stanford Daily, 436 U.S. 547 (1978).
[46] Fisher v. United States, 425 U.S. 391 (1976).

records, unless the records are legally exempt."[47] The Privacy Act applies only to the federal government and has not been expanded to include records kept by the private sector. In 1986, the Electronic Communications Privacy Act (EPCA) restricted wiretapping, regulated government access to electronic communication stored by third parties, and prohibited the collection of communications content (i.e., what was said, not who was called) by pen registers. After the Supreme Court ruled in the 1976 case *United States v. Miller* that there was no reasonable expectation of privacy for records at financial institutions, Congress passed The Right to Financial Privacy Act,[48] which extended Fourth Amendment protections to these records. As required by the 1996 Health Insurance Portability and Accountability Act (HIPAA), in 2002 the Department of Health and Human Services published the final form of "the Privacy Rule," which set the "standards for the electronic exchange, privacy and security of health information."[49] This accumulation of privacy protections includes laws covering specific sectors—or responding to specific events—but not any overarching design. A well-known case in point is Congress' enactment of The Video Privacy Protection Act after the

[47] *Privacy Act of 1974, as amended*, FEDERAL TRADE COMMISSION, available at: http://www.ftc.gov/foia/privacy_act.shtm (accessed April 7, 2013).
[48] The Right to Financial Privacy Act of 1978, 12 U.S.C. §§ 3401-342.
[49] Summary of the HIPAA Privacy Rule, Department of Health and Human Services, http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/

video rental records of Supreme Court nominee Judge Robert Bork were obtained by a Washington, D.C. newspaper.[50]

Congress could help to establish a privacy doctrine for the cyber age by reviewing what by now has been fairly called an incomplete "patchwork of federal laws and regulations" and providing a comprehensive overall ranking of protections based on the sensitivity of the data.[51]

b. Volume

The second dimension that a cyber age privacy doctrine should draw on is the volume of information collected. Volume refers the total amount of information collected about the same person holding constant the level of sensitivity. Volume reflects the extent of time surveillance is applied (the issue raised in *Jones*); the amount of information collected at each point in time (e.g., just emails sent to a specific person or all emails stored on a hard drive?); the bandwidth of information collected at any one point in time (e.g., only the addresses of email sent or also their content?). A single piece of low-sensitivity data deserves the least protection, and a high volume of sensitive information should receive the most protection.

[50] The Video Privacy Protection Act of 1988, 18 U.S.C. § 2710

[51] Gina Stevens, *Privacy Protections for Personal Information Online*, Congressional Research Service, Apr. 6, 2011.

Under such a cyber age privacy doctrine, different surveillance and search technologies differ in their intrusiveness. Least intrusive are those which collect only discreet pieces of information of the least sensitive kind. These include speed detection cameras, toll booths, and screening gates, because they all reveal, basically, one piece of information of relatively low sensitivity. Radiation detectors, heat reading devices and bomb and drug-sniffing dogs belong into this category, not only because of the kind of information (low or not sensitive) they collect, but also because the bandwidth of the information they collect is very low (just one facet, indeed a very narrow one, and for a short duration).

Typical CCTVs—privately owned, mounted on one's business, parking lot, or residential lobby—belong into the middle range because they pick up several facets (location, physical appearance, who one associates with), but do so only for only a brief period of time and in one locality. The opposite holds for Microsoft's Domain Awareness System, first tested in New York City in 2012. The program makes public data—like that from the city's 3,000 CCTV cameras, arrest records, 911 calls, license plate readers, and radiation detectors—easily and instantly accessible to the police. While the system does not yet utilize facial recognition, it could be readily expanded to include such technology.

Phone tapping—especially if not minimized (see below) and continued for extended period of time—and computer searches, collect more volume. (This

should not be conflated with considerations that come under the third dimension, whether these facts are stored, collated, analyzed and distributed, i.e., the elements of cybernation.)

Drones are particularly intrusive because they involve much greater bandwidth and have the potential to engage in very prolonged surveillance at relatively low costs (compared to, say, a stake out).

These volume rankings must be adapted as technologies change. The extent to which combining technologies is intrusive depends on the volume (duration and bandwidth, holding sensitivity constant) collected.

When the issue of extending privacy protection beyond spot collection arose in *Jones*, several legal scholars, in particular Orin Kerr, pointed to the difficulties in determining when the volume of collection was reasonable and when it became excessively intrusive. Kerr writes: "In *Jones*, the GPS device was installed for 28 days. Justice Alito stated that this was 'surely' long enough to create a mosaic. But he provided no reason why, and he recognized that 'other cases may present more difficult questions.' May indeed. If 28 days is too far, how about 21 days? Or 14 days? Or 3.6 days? Where is the line?"[52] In response, one notes that there are numerous such cut off points in law, such as the number of days suspects may be detained before must be charged or released, the voting and driving age, the

[52] *Id.* at 24.

number of jurors and so on. One may say that they reflect what a "reasonable" person would rule. Actually they reflect what judges consider a compromise between a restriction that is clearly excessive and clearly inadequate—a line that has been adjusted often. There is no reason the volume of collection should not be similarly governed.

c. Cybernation: Storing, analysis, and access

The third dimension seems to be the one that is increasing in importance and regarding which law and legal theory have the most catching up to do. To return to the opening deliberations, historically, much attention was paid to the question whether the government can legally collect certain kinds of information under specific conditions. This was reasonable because most violations of privacy occurred through search and surveillance that implicated this first-level collection of spot information. True, some significant violations also occurred as a result of collating information, storing it, analyzing it and distributing it. However, to reiterate, as long as records were paper bound, which practically all were, these secondary violations of privacy were inherently limited when compared to those enabled by the digitization of data and the use of computers, i.e., by cybernation.

To illustrate this cardinal transformative development, a comparison: In one state, a car passes through a tollbooth, a picture of its license plate is taken—and then this information is immediately deleted from the computer if the proper

payment is made. In another state, the same information, augmented with a photo of the driver, is automatically transmitted to a central data bank. Here, it is combined with many thousands of other pieces of information about the same person, from locations he has visited (based on cell tower triangulation) to his magazine subscriptions, recent purchases and so on. The information is regularly analyzed by artificial intelligence systems to determine if people are engaged in any unusual behavior, what places of worship they frequent (flagging Mosques), which political events they attend (flagging those who are often involved in protests), and if they stop at gun shows. The findings are widely distributed to local police and the intelligence community, and can be gained by the press and divorce lawyers.

Both systems are based on spot information; that is, pieces of information pertaining to a very limited, specific event or point in time and typically of little significance in themselves—as in the case in the first state. However, if such information is combined, analyzed, and distributed, as depicted in the second scenario, it provides a very comprehensive and revealing profile of one's personal life. In short, the most serious violations of privacy are often perpetuated not by surveillance or information collection per se, but by combination, manipulation, and data sharing—by cybernation. The more information is cybernated, the more intrusive it becomes.

## Part III. Limiting intrusion by cybernation

There are in place two major systematic approaches to deal with privacy violations that result from secondary uses, namely the third party doctrine and the EU Data Protection Directive (DPD). The third party doctrine holds that once a person voluntarily discloses a fact to another party, that party is free to pass on (or sell) this information to third parties and the various parties are free to further process this information, collate it with other data, draw inferences and so on—in short, to cybernate it.[53]

This approach is challenged by critics who note that in the cyber age much of our private lives are lived in a cyber world operated by third parties like Google and Facebook. Thus, Matthew Lawless writes that,

> "the third party doctrine gives effect to the criticism often aimed at the 'reasonable expectation of privacy' principle, by holding that individuals can only reasonably expect privacy where the Court gives them that privacy. Because the third party doctrine fails to address true societal expectations of privacy (as evident by its failure to protect any information entered into a search engine), it reinforces the privacy norms of a politically and temporally insulated judiciary: once people know their searches are exposed, then—by the time these cases are contested—there will, in truth, be no expectation of privacy."[54]

---

[53] Information voluntarily handed over to another party does not receive Fourth Amendment protection "even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed." United States v. Miller, 425 U.S. 435, 443 (1976); *see also* Orin Kerr, *The Case for the Third Party Doctrine*, 107 MICH. L. REV. 561, 569–70 (2009). Earlier cases that built up this doctrine include Lee v. United States 343 U.S. 747 (1952); Couch v. United States 409 U.S. 322 (1973).

[54] Matthew D. Lawless, *The Third Party Doctrine Redux: Internet Search Records and the Case for a "Crazy Quilt" of Fourth Amendment Protection*, 2 UCLA J.L. & TECH. 1 (2007)

However, even without drawing on whatever the societal expectation of privacy is, one notes that considerable harm will come to people and that core societal values would be violated, if the third party doctrine is given free rein. This observation is strengthened by the fact that various exceptions to the third party doctrine are already in place, for instance special rules for medical and financial information. However, according to Greg Nojeim, these rules do not provide the same level of protection granted by the Fourth Amendment protection. He notes that "privacy statutes that protect some categories of sensitive personal information generally do not require warrants for law enforcement access."[55] Furthermore, Matthew Tokson argues that "The conflation of disclosure to automated Internet systems with disclosure to human beings" has led the court to exclude a great deal of personal information from Fourth Amendment protection, including "Internet protocol ("IP") addresses, e-mail to/from information, information about the volume of data transmitted to a user, name, address, and credit card information, and even the contents of a user's e-mails."[56]

The European Union's DPD in effect takes the opposite view, namely that any secondary use of personal information released by the person or collected about him requires the explicit *a priori* approval of the original individual 'owner'

---

[55] Orin Kerr and Greg Nojeim, *The Data Question: Should the Third-Party Records Doctrine Be Revisited?*, ABA J., August 1, 2012, available at: http://www.abajournal.com/magazine/article/the_data_question_should_the_third-party_records_doctrine_be_revisited/.

[56] Matthew Tokson, *Automation and the Fourth Amendment*, 96 IOWA L. REV. 581, 586 (2011).

of the information, and that this consent cannot be delegated to an agent or machine.[57] The details of DPD are complex and changing.[58] For instance, it made exceptions for many areas from this rule, for instance when the data are needed for research, public health, or law enforcement, among others. In January 2012, the European Commission passed draft legislation that would update the existing data protection law. This legislation includes an 'opt in' provision: "As a general rule, any processing of personal data will require providing clear and simple information to concerned individuals as well as obtaining specific and explicit consent by such individuals for the processing of their data." Data show that information about a person is used many times each day by a large variety of users. Hence, if such a policy were systematically enforced, each Internet user would have to respond to scores if not hundreds of requests per day even for uses of non-sensitive information. It seems that in this area, as in many others, the way DPD rules survive is by very often not enforcing them. Whenever I meet Europeans, and following public lectures in the EU, I ask if anyone has been ever asked to consent to the use of personal information that they had previously released. I have found only one person so far. He said that he got such a request—from Amazon. Other

[57] Daniel Cooper, *Consent in EU Data Protection Law*, EUROPEAN PRIVACY ASSOCIATION, available at http://www.europeanprivacyassociation.eu/public/download/EPA%20Editorial_%20Consent%20in%20EU%20Data%20Protection%20Law.pdf (accessed April 7, 2013).

[58] *Why do we need an EU data protection reform?*, EUROPEAN COMMISSION, available at http://ec.europa.eu/justice/data-protection/document/review2012/factsheets/1_en.pdf (accessed April 7, 2013).

sources indicate that compliance is, at best, "erratic".[59] The penalties for violating the DPD seem to be miniscule and rarely collected. No wonder a large majority of the EU public—70 percent—fear that their personal data may be misused.[60]

In short, neither of these approaches is satisfactory.

In addition, there are in place a large number of laws, regulations, and guidelines that deal with limited particular usages of personal information beyond the collection point. However (a) a very large number of them deal with only one dimension of the cube, and often only with one element of cybernation, limiting either storage, or analysis, or distribution. (b) They reflect the helter-skelter way they were introduced, and do not provide a systematic doctrine of cyber privacy. They are best viewed as building blocks, which, if subjected to considerable legal scholarship and legislation, could provide the needed doctrine. They are like a score of characters in search of an author.

One of the key principles for such a doctrine is that the legal system can be more tolerant of the primary point spot collection of personal information (a) the more limited the volume (duration and bandwidth) of the collection[61] and (b) the

---

[59] Erica Newland, "CDT Comments on EU Data Protection Directive," Center for Democracy and Technology, January 20, 2011, https://www.cdt.org/blogs/erica-newland/cdt-comments-eu-data-protection-directive

[60] "Data protection reform: Frequently asked questions," Europa, January 25, 2012, http://europa.eu/rapid/press-release_MEMO-12-41_en.htm?locale=fr.

[61] In the wake of *Jones*, Professor Susan Freiwald identified four factors that the courts use to extend Fourth Amendment protection to new surveillance technologies that "make sense." These include whether the target is unaware of the surveillance; it covers items that the people consider private; it is continuous; and it is indiscriminate (covers more information than is necessary for establishing guilt). Susan Freiwald, *The Four Factor Test*, THE SELECTED WORKS OF SUSAN FREIWALD, available at: http://works.bepress.com/susan_freiwald/11.

more limited and regulated cybernation is—holding constant the level of sensitivity of the information. (That is, much more latitude can be granted to the collection and cybernation of insensitive information, stricter limitation on highly sensitive information, and a middle level of protection in between). The same holds for the threat level to the common good.

In other words, a cyber age privacy doctrine can be much more tolerant of primary collection conducted within a system of laws and regulations that are effectively enforced to ensure that cybernation is limited, properly supervised, and employed for legitimate purposes —and much less so, if the opposite holds. One may refer to this rule as the inverse relationship between primary license and secondary constraints.

Another key principle is a ban on using insensitive information to divine the sensitive—e.g., using information about routine consumer purchases to divine one's medical condition—because it is just as intrusive as collecting and employing sensitive information.[62] This is essential because currently such behavior is rather common.[63] Thus, under the suggested law, Target would be

---

[62] People often trust assurances that their sensitive information (names and social security number) can be deleted when their data is collected in large databases. In fact, scientists have shown that individuals can be easily "deanonymized." Paul Ohm writes that this misunderstanding has given the public a false sense of security and has lead to inadequate privacy protections, laws and regulations. *See* Peter Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. Rev. 1701 (2010). *See also* Marcia Stepanek, *Weblining*, BusinessWeek, April 3, 2000, at http://www.businessweek.com/2000/00_14/b3675027.htm; Jennifer Golbeck, Christina Robles & Karen Turner, *Predicting Personality with Social Media*, CHI EXTENDED ABSTRACTS 2011, 253-262.

[63] Marcy Peek, Passing Beyond Identity on the Internet: Espionage and Counterespionage in the Internet Age, 28 VT. L. REV. 91, 94 (2003) (evaluating ways to resist discriminatory marketing in cyberspace); Marcia Stepanek,

prevented from sending coupons for baby items to a teenage girl after the chain store's analysis of her recent purchases suggested she might be pregnant.[64]

Kerr correctly points out that it would be exceedingly difficult to cover the private sector by drawing on the Fourth Amendment and points, instead, to the 1986 Electronic Communications Privacy Act (ECPA) to show that Congress can enact laws that protect people from intrusion both by the government and by private actors.[65] To further advance the cyber age privacy doctrine, much more attention needs to be paid to private actors. Privacy rights, like others, are basically held against the government, to protect people from undue intrusion by public authorities. However, increasingly cybernation is carried out by the private sector. There are corporations that make shadowing Internet users—and keeping very detailed dossiers on them—their main line of business. According to Slobogin,

> "Companies like Acxiom, Docussearch, ChoicePoint, and Oracle can provide the inquirer with a wide array of data about any of us, including: basic demographic information, income, net worth, real property holdings, social security number, current and previous addresses, phone numbers and fax numbers, names of neighbors, driver records, license plate and VIN numbers, bankruptcy and debtor filings, employment, business and criminal

---

Weblining, BUS. WK., Apr. 3, 2000, http://www.businessweek.com/2000/00_14/b3675027.htm (A data broker company Acxiom matches names against housing, education, and incomes in order to identify the unpublicized ethnicity of an individual or group.); Nicholas Carr, Tracking Is an Assault on Liberty, With Real Dangers, WALL ST. J., Aug. 7–8, 2010, at W1 ("It used to be . . . you had to get a warrant to monitor a person or a group of people. Today, it is increasingly easy to monitor ideas."); Amitai Etzioni, *Privacy Merchants: What Is To Be Done?*, 14 PENN. J. CONST. L, 929, 948-950 (2012).

[64] *How Target Figured Out A Teen Girl Was Pregnant Before Her Father Did*, FORBES, Feb. 16, 2012, http://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did/

[65] Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801, 871–2 (2004).

> records, bank account balances and activity, stock purchases, and credit card activity."[66]

And these data are routinely made available to the government, including the FBI. Unless this private cybernation is covered, the cyber age privacy doctrine will be woefully incomplete.[67]

Given that private actors are very actively engaged in cybernation and often tailor their work so that it might be used by the government (even if no contract is in place and they are, hence, not subject to the limits imposed on the government), extending privacy doctrine beyond the public/private divide is of pivotal importance for the future of privacy in the cyber age. Admittedly, applying to the private sector similar restrictions and regulations that control the government is politically unfeasible. However, as one who analyzes the conditions of society from a normative viewpoint, I am duty bound to point out that it makes ever less sense to maintain this distinction.[68] Privacy will be increasingly lost in the cyber age, with little or no gain to the common good, unless private actors—and not just the government—are more reined in. To what extent this may be achieved by self regulation, changes in norms, increased transparency, or government regulation is a question not here addressed.

---

[66] Christopher Slobogin, *Government Data Mining and the Fourth Amendment*, 75 U. CHI. L. REV. 317, 320 (2008).

[67] For further discussion on these matters, see Amitai Etzioni, *The Privacy Merchants: What Is To Be Done?*, 14 PENN. J. CONST. L. 929 (March 2012); Amitai Etzioni, *The Bankruptcy of Liberalism and Conservatism*, 128 PSQ 39 (2013) (discussing the collapse of the public-private divide).

[68] For more discussion, see Amitai Etzioni, *The Bankruptcy of Liberalism and Conservatism*, 128 PSQ 39 (2013).

For this doctrine to be further developed laws and court rulings ought to be three dimensional.[69] These laws and court cases best specify not merely whether a particular collection of personal information is a 'search,' but also what level of sensitivity can be tolerated and to what extent the information may be stored, massaged, and distributed. This may seem—and is—a tall, if not impossible, order. However, as is next illustrated, a considerable number of measures are already in place that are, in effect, at least two dimensional. These, though, suffer from the fact that they have been introduced each on their own and do not reflect an overarching doctrine of privacy and, hence, reveal great inconsistencies that need to be remedied. I cannot stress enough that the following are but selective examples of such measures.

One should note that a very early attempt to deal with the issue—basically, in terms here used, by banning a form of cybernation—utterly failed. In 2003, Congress shut down the Pentagon's "Total Information Awareness" program, which was created to detect potential terrorists by using data mining technologies to analyze unprecedented amounts personal transaction data. However, a report by the *Wall Street Journal* in 2008 revealed that the most important components of

[69] Kerr sees a greater role here for Congress, while Swire for the courts. *See* Peter P. Swire, *Katz is Dead. Long Live Katz,* 102 MICH. L. REV. 904, 912 (2002) and Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution,* 102 MICH. L. REV. (2004). This article is unable to add to these deliberations other than to recognize that both are needed and neither seems able to keep up with changing technologies.

T.I.A. were simply "shifted to the NSA" and "put in the so-called black budget, where it would receive less scrutiny and bolster other data-sifting efforts."[70]

Minimization is one way of addressing the volume issue as Swire pointed out in his groundbreaking article on *Jones* and mosaic theory.[71] Accordingly, when the FBI taps a phone, even for an extended period of time, the intrusion can be reduced significantly if the FBI either stops listening when it hears that the conversation is not relevant to the investigation (e.g., a child is calling the suspect under surveillance) or lock away those segments of the taped correspondence that turn out to be irrelevant.[72] For this rule to be integrated into the doctrine, it may be waived for insensitive information. That is, there would be no need to minimize if the child asked, say, to watch TV, but activated if she asked, say, about the medical news about a family member.

Another example of a safeguard against excessive privacy intrusions is the requirement that certain content be deleted after a specific time period. Most private companies that utilize CCTV erase video footage after a set number of days, for instance after a week. Admittedly, their reasons for doing so may be simply economic; however the effect is still to limit the volume of collection and potential for subsequent abuse. Note that that there are no legal requirements to

---

[70] Siobhan Gorman, *NSA's Domestic Spying Grows As Agency Sweeps Up Data,* WALL STREET J., Mar. 10, 2008.
[71] Peter P. Swire, A *Reasonableness Approach to Searches After the Jones GPS Tracking Case,* 64 STAN. L. REV. ONLINE 57 (2012).
[72] Gary T. Marx, *Ethics for the New Surveillance,* 14 THE INFORMATION SOCIETY: AN INTERNATIONAL JOURNAL 171, 178 (1998).

erase these tapes. However, such laws ought to be considered. (Europeans are increasingly recognizing a “right to be forgotten.”) It would be in the public interest to require that footage be kept for a fixed period of time (as it has proven useful in fighting crime and terrorism), but also ban under most circumstances the integration of the video feed into encompassing and cybernated systems, of the kind Microsoft has developed (discussed above).

The treatment of private local CCTVs should be examined in the context of the ways other such spot collection information is treated. Because the bandwidth of information collected by tool booths, speed cameras and radiation detectors is very narrow, one might be permitted to store it longer and feed it into cybernated systems. By contrast, cell phone tracking can be utilized to collect a great volume and bandwidth of information about a person’s location and activities. People carry their phones to many places they cannot take their cars, where no video cameras or radiation detectors will be found, including sensitive places such as political meetings, houses of worship, and residences. (These rules must be constantly updated as what various technologies can observe and retain, constantly changes.)

Regulations to keep information paper bound have been introduced for reasons other than protecting privacy, but these requirements still have the effect of limiting intrusiveness. For example, Congress prevents the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF) from computerizing gun records when

such information is collected during background checks.[73] In 2013, an amendment to the anti-insider trading STOCK Act exempted 28,000 executive branch staff from having to post their financial disclosure forms "online in a searchable, sortable and downloadable format."[74] These bans remind one, that not all the privacy measures that are in place are legitimate and that some are best scaled back rather than enhanced.[75]

A related issue is raised by the cybernation of arrest records. Arrest records should be, but are not, considered highly-sensitive information. When these records, especially those concern people who were subsequently released without any charges, were paper bound, the damage they inflicted on most people's reputations was limited. However, as a result of cybernation, they have become much more problematic. Under the suggested doctrine, arrest records of people not charged after a given period of time would be available only to law enforcement officers. The opposite might be said about data banks that alert the public to physicians that have been denied privileges for cause, a very high threshold that indicates serious ethical shortcomings.

Many computer systems ("clouds" included) encrypt their data and a few have introduced audit trails. The cyber age privacy doctrine might require that all

---

[73] Erica Goode and Sheryl Gay Stolberg, *Legal Curbs Said to Hamper A.T.F. in Gun Inquiries*, N.Y. TIMES, Dec. 25, 2012.
[74] Tamara Keith, *How Congress Quietly Overhauled Its Insider-Trading Law*, NPR, Apr. 16, 2013, http://m.npr.org/news/Politics/177496734.
[75] AMITAI ETZIONI, THE LIMITS OF PRIVACY (2000).

data banks that contain sensitive information be encrypted and include at least some rudimentary form of an audit trail.

Technologies can be recalibrated to collect the 'need to know' information while shielding extraneous but highly sensitive, information from observation. For example, when law enforcement collects DNA samples from convicted criminals or arrested individuals, FBI analysts create DNA profiles using so-called 'junk DNA' "because it is not 'associated with any known physical or medical characteristics,' and thus theoretically poses only a minimal invasion of privacy."[76] Storing these "genetic fingerprints" in national databases is much less intrusive than retaining data produced by blood samples, which reveal "reveal sensitive medical or biological information."[77] In 2013, the TSA stopped its use of body scanners that revealed almost nude images, using instead scanners that produce "cartoon-like" images, on which the scanners mark places hidden objects are found.[78] This did not affect the volume of collection, but lessened the sensitivity of the content.

Other measures must address the fact that often data can be "re-identified" or "de-anonymized." In 2006, AOL released the search records—stripped of "personal identifiers"—of over 600,000 people. An investigation by the *New York*

---

[76] Anna C. Henning, *Compulsory DNA Collection: A Fourth Amendment Analysis*, CONGRESSIONAL RESEARCH SERVICE R40077, at 2, Feb. 16, 2010.
[77] *Id.* at 13.
[78] Jack Nicas, TSA to Halt Revealing Body Scans at Airports, WALL STREET JOURNAL, Jan. 18, 2013.

*Times*, however, demonstrated that intimate information—including names and faces—can be gleaned from such purportedly anonymous data. This risk is mitigated by the development of statistical methods that prevent such undertakings, such as "differential privacy," which allows curators of large databases to release the results of socially beneficial data analysis without compromising the privacy of the respondents who make up the sample.[79]

Many more examples could be provided. However, the above list may suffice to show that, while there are numerous measures in place that deal with various elements of the privacy cube, these have not been introduced with systematic attention to the guiding principles needed for the cyber age.

[79] Cynthia Dwork, *Differential Privacy: A Survey of Results*, in M. Agrawal et al. (Eds.): TAMC, LNCS 4978, pp. 1–19 (2008) (Roughly speaking, differential privacy ensures that the removal or addition of a single database item does not (substantially) affect the outcome of any analysis. It follows that no risk is incurred by joining the database, providing a mathematically rigorous means of coping with the fact that distributional information may be disclosive.").