



2014

Bulk Metadata Collection: Statutory and Constitutional Considerations


Laura K. Donohue

Georgetown University Law Center, lkdonohue@law.georgetown.edu

This paper can be downloaded free of charge from:
<https://scholarship.law.georgetown.edu/facpub/1350>
<http://ssrn.com/abstract=2344774>

37 Harv. J.L. & Pub. Pol'y 757-900 (2014)

This open-access article is brought to you by the Georgetown Law Library. Posted with permission of the author.
Follow this and additional works at: <https://scholarship.law.georgetown.edu/facpub>

 Part of the [Comparative and Foreign Law Commons](#), [Constitutional Law Commons](#), [First Amendment Commons](#), [Fourth Amendment Commons](#), and the [National Security Law Commons](#)

BULK METADATA COLLECTION: STATUTORY AND CONSTITUTIONAL CONSIDERATIONS

PROFESSOR LAURA K. DONOHUE*

INTRODUCTION	759
I. BULK COLLECTION IN THE CONTEXT OF FISA'S	
GENERAL APPROACH.....	766
A. Prior Domestic Surveillance.....	767
1. NSA Programs.....	770
a. Project MINARET.....	772
b. Operation SHAMROCK.....	773
2. Broader Context	776
B. Protections Built into FISA.....	782
1. Entity Targeted Prior to Acquisition....	784
2. Probable Cause and Showing of Criminal Wrongdoing Prior to Collection	786
3. Minimization Procedures for Acquisition and Retention.....	791
4. Establishment of the Foreign Intelligence Surveillance Court and Court of Review	792
C. Subsequent Amendment.....	793
1. Physical Search, Pen-Trap	794

* Professor of Law, Georgetown University Law Center. Christine Ciambella was invaluable in obtaining research materials. My appreciation also extends to the members of the *Harvard Journal of Law & Public Policy* for their edits on the final Article. Special thanks to Hope Babcock, Bill Banks, Julie Cohen, George Jameson, Allegra MacLeod, Julie O'Sullivan, Milton Regan, Tanina Rostain, Kim Lane Scheppele, and Mike Seideman, for their comments on an earlier draft of this Article. In October 2013 an early version of this Article was placed online. Steve Vladeck, *Laura Donohue's Comprehensive Case Against Bulk Metadata Collection*, JUST SECURITY (Oct. 23, 2013, 6:32 PM), <http://justsecurity.org/2013/10/23/laura-donohues-comprehensive-case-bulk-metadata-collection/>, [<http://perma.cc/S6G5-FMTM>]; see also *Continued Oversight of the Foreign Intelligence Surveillance Act: Hearing Before the S. Comm. On the Judiciary*, 113th Cong. (2013) (statement of Laura K. Donohue, Professor of Law, Georgetown University Law Center).

2.	Business Records, Tangible Goods, and Section 215.....	797
D.	Broad Surveillance in Place of Particularization	803
1.	Wholesale Collection of Information ...	803
2.	Absence of Prior Targeting.....	805
3.	No Higher Threshold for U.S. Persons	806
E.	Role of the Foreign Intelligence Surveillance Court.....	806
1.	Reliance on NSA to Ascertain Reasonable, Articulate Suspicion	807
a.	Failure to Report Initial Noncompliance.....	808
b.	Further Noncompliance	814
c.	FISC Response	817
d.	Technological Gap.....	821
2.	Issuance of Detailed Legal Reasoning and Creation of Precedent	822
3.	Judicial Design	825
a.	Appointments	825
b.	Order Rate	831
II.	BULK COLLECTION AND FISA'S STATUTORY PROVISIONS.....	836
A.	"Relevant to an Authorized Investigation"	836
1.	Relevance Standard	838
2.	Connection to "an Authorized Investigation"	843
a.	Collection of the Information	843
b.	Specificity	847
c.	Future Authorized Investigations..	848
B.	Subpoena Duces Tecum	850
1.	Fishing Expeditions	853
2.	Specificity	854
3.	Past Crimes	856
4.	March 2009 FISC Opinion.....	857
C.	Evisceration of Pen-Trap Provisions.....	858
D.	Potential Violation of Other Provisions of Criminal Law	860

III. CONSTITUTIONAL CONSIDERATIONS.....	863
A. The Problem with <i>Smith v. Maryland</i>	865
B. More Intrusive Technologies and Their Impact on Privacy.....	871
C. Judicial Tension: Trespass and <i>Katz's</i> Reasonable Expectation of Privacy	874
1. The Prohibition on General Warrants.....	875
2. Search of Metadata and the Reasonable Expectation of Privacy.....	884
D. The Proverbial Needle in the Haystack.....	892
IV. CONCLUSION	897

INTRODUCTION

On May 24, 2006, the Foreign Intelligence Surveillance Court (FISC) approved an FBI application for an order, pursuant to 50 U.S.C. § 1861, requiring Verizon to turn over all telephony metadata to the National Security Agency.¹ The Court subsequently approved similar applications for all major U.S. telecommunication service providers. Over the next seven years, FISC issued orders renewing the bulk collection program thirty-four times.² Almost all of the information obtained related to

1. *In re* Application of the Fed. Bureau of Investigation for an Order Requiring the Prod. of Tangible Things from [Telecommunications Providers] Relating to [REDACTED], Order, No. BR 0605 (FISA Ct. May 24, 2006), available at https://www.eff.org/sites/default/files/filenode/docket_06-05_1dec201_redacted.ex_-_ocr_0.pdf, [http://perma.cc/MT9D-4W2Y] (released by court order as part of the Electronic Frontier Foundation's Freedom of Information Act (FOIA) litigation). Note that the specific telecommunications companies from which such records were sought were redacted, as well as the remaining title; the government, however, also released an NSA report that provided more detail on the title of the Order. OFFICE OF THE INSPECTOR GEN., NAT'L SEC. AGENCY, ST-06-0018, ASSESSMENT OF MANAGEMENT CONTROLS FOR IMPLEMENTING THE FOREIGN INTELLIGENCE SURVEILLANCE COURT ORDER: TELEPHONY BUSINESS RECORDS, available at http://www.dni.gov/files/documents/section/pub_Feb%2012%202009%20Memorandum%20of%20US.pdf, [http://perma.cc/YXA7-PTT4] (see page 94 of 1846 and 1862 Production). For purposes of a more precise citation, I draw from both sources.

2. ADMINISTRATION WHITE PAPER: BULK COLLECTION OF TELEPHONY METADATA UNDER SECTION 215 OF THE USA PATRIOT ACT 2 (Aug. 9, 2013), available at <https://www.documentcloud.org/documents/750211-administration-white->

the activities of law-abiding persons who were not the subjects of any investigation.³

This program remained secret until mid-2013, when a combination of leaks by Edward Snowden, a former National Security Agency (NSA) employee, and Freedom of Information Act litigation launched by the Electronic Frontier Foundation, forced key documents into the public domain.⁴ In response, the Obama Administration issued statements, fact sheets, redacted FISC opinions, and even a White Paper, acknowledging the existence of the program and arguing that it is both legal and constitutional.⁵

According to these documents, the purpose of the telephony metadata program is to collect information related to counterterrorism efforts and foreign intelligence.⁶ These data include all communications routing information, including (but not limited to) session identifying information (for example, originating and terminating telephone number, identity of the communications device, etc.), trunk identifier, and time and duration of the call.⁷ The metadata collected as part of this program does not include the substantive content of communica-

paper-section-215.html, [<http://perma.cc/V7VM-5MAU>] [hereinafter SECTION 215 WHITE PAPER].

3. *In re* Prod. of Tangible Things From [REDACTED], No. BR 08-13, at 12 (FISA Ct. Mar. 2, 2009), available at http://www.dni.gov/files/documents/section/pub_March%202%202009%20Order%20from%20FISC.pdf, [<http://perma.cc/5LYL-RKAZ>].

4. *Electronic Frontier Found. v. Dep't of Justice*, No. 4:11-cv-05221-YGR, at 2, ¶ 1(b) (N.D. Cal. Jul. 19, 2013) (order responding to the request for records related to Section 215, i.e., orders and opinions of the FISC issued from January 1, 2004 to June 6, 2011, containing a significant legal interpretation of the government's authority or use of its authority under Section 215; and responsive "significant documents, procedures, or legal analyses incorporated into FISC opinions or orders and treated as binding by the Department of Justice or the National Security Agency").

5. See, e.g., *In re* Application of the Fed. Bureau of Investigation for an Order Requiring the Prod. of Tangible Things from [Telecommunications Providers] Relating to [REDACTED], Order, No. BR 0605 (FISA Ct. May 24, 2006), available at https://www.eff.org/sites/default/files/filenode/docket_06-05_1dec201_redacted.ex_-_ocr_0.pdf, [<http://perma.cc/MT9D-4W2Y>] (released by court order as part of the Electronic Frontier Foundation's Freedom of Information Act (FOIA) litigation); SECTION 215 WHITE PAPER, *supra* note 2, at 2.

6. See, e.g., SECTION 215 WHITE PAPER, *supra* note 2, at 3 ("The Government cannot conduct substantive queries of the bulk records for any purpose other than counterterrorism."); *id.* at 4 ("Query results can be further analyzed only for valid foreign intelligence purposes.").

7. *Id.* at 3.

tions, nor does it include subscribers' names, addresses, or financial information.⁸

Although many of the details about the telephony metadata program remain classified, from what has been made public by the government, it appears that the NSA takes all information obtained and feeds it into a bulk data set, which is then queried with an "identifier," referred to as a "seed."⁹ The NSA uses both international and domestic identifiers.¹⁰ FISC requires that the NSA establish a "reasonable, articulable suspicion" that a seed identifier used to query the data is linked to a foreign terrorist organization before running it against the bulk data. Once obtained, information responsive to the query can be further mined for information. The NSA can analyze the data to ascertain second- and third-tier contacts, in steps known as "hops."¹¹

8. Content is defined consistent with 18 U.S.C. § 2510(8) (2006). But note that the same arguments brought by the government in support of the telephony metadata program would support building similar databases of subscribers' and customers' financial records. See SECTION 215 WHITE PAPER, *supra* note 2, at 3. In addition, the *Section 215 White Paper* is careful to note that the government does not collect cell phone locational information "pursuant to these orders." *Id.* However, the same arguments that support the telephony metadata program would support the collection of precisely this information under other FISC orders.

9. SECTION 215 WHITE PAPER, *supra* note 2, at 3. Note that although the White Paper uses telephone numbers as an example of an identifier, it is conceivable that various other identifiers may be used. In a recently-released memorandum, for instance, the government refers to "bins" or "zip codes," suggesting that the types of queries can be significantly broad. See Memorandum of the United States in Response to the Court's Order Dated Jan. 28, 2009 at 9, *In re Prod. of Tangible Things from [REDACTED]*, No. BR 08-13 (FISA Ct. Feb. 17, 2009), available at http://www.dni.gov/files/documents/section/pub_Feb%2012%202009%20Memorandum%20of%20US.pdf, [<http://perma.cc/9EYZ-D597>]. The Guardian, in turn, reports that the term "identifiers" includes information such as names, telephone numbers, e-mail addresses, IP addresses, and usernames. See James Ball & Spencer Ackerman, *NSA loophole allows warrantless search for U.S. Citizens' emails and phone calls*, THE GUARDIAN, Aug. 9, 2013, <http://www.theguardian.com/world/2013/aug/09/nsa-loophole-warrantless-searches-email-calls>, [<http://perma.cc/UVP5-TCJJ>] (containing screen shot of classified document).

10. Memorandum of the United States in Response to the Court's Order Dated Jan. 28, 2009 at 8, 10, *In re Prod. of Tangible Things From [REDACTED]*, No. BR 08-13 (FISA Ct. Feb. 17, 2009), available at http://www.dni.gov/files/documents/section/pub_Feb%2012%202009%20Memorandum%20of%20US.pdf, [<http://perma.cc/9EYZ-D597>].

11. SECTION 215 WHITE PAPER, *supra* note 2, at 3-4 ("The first 'hop' refers to the set of numbers directly in contact with the seed identifier. The second 'hop' refers to the set of numbers found to be in direct contact with the first 'hop' numbers, and the third 'hop' refers to the set of numbers found to be in direct contact with the second

As a practical matter, the NSA interprets the primary order as authorizing the agency to retrieve information as many as three tiers away from the initial identifier.¹² The government refers to this process as “automated chaining.”¹³ These results can then be further queried for “foreign intelligence purposes.”¹⁴ In some cases, this information can then be forwarded to the FBI for further investigation, including using the information for an application for an electronic intercept order under Title I of the Foreign Intelligence Surveillance Act.¹⁵ On at least three occasions, the government has obtained authorization to expand the telephone identifiers that the NSA could query.¹⁶

‘hop’ numbers.”). Initially, neither FISC nor the NSA limited the number of ‘hops’ that could be undertaken. In March 2009, the government implemented software changes to its system to limit the number of hops permitted to three. Memorandum of the United States in Response to the Court’s Order Dated Jan. 28, 2009 at 20, *In re Prod. of Tangible Things From [REDACTED]*, No. BR 08-13 (FISA Ct. Feb. 17, 2009), available at http://www.dni.gov/files/documents/section/pub_Feb%2012%202009%20Memorandum%20of%20US.pdf, [http://perma.cc/9EYZ-D597]. In January 2014 the President announced that henceforward the number of hops would be limited to two. *Transcript of President Obama’s Jan. 17 speech on NSA reforms*, WASH. POST, Jan. 17, 2014, http://www.washingtonpost.com/politics/full-text-of-president-obamas-jan-17-speech-on-nsa-reforms/2014/01/17/fa33590a-7f8c-11e3-9556-4a4bf7bcb84_story.html, [http://perma.cc/CF5-TVP5] (“Effective immediately, we will only pursue phone calls that are two steps removed from a number associated with a terrorist organization, instead of the current three.”). Notably, these changes are not statutory; nor are there statutory provisions requiring that the number of hops, should it be changed, be made public.

12. SECTION 215 WHITE PAPER, *supra* note 2, at 4.

13. Memorandum of the United States in Response to the Court’s Order Dated Jan. 28, 2009 at 10, *In re Prod. of Tangible Things From [REDACTED]*, No. BR 08-13 (FISA Ct. Feb. 17, 2009), available at http://www.dni.gov/files/documents/section/pub_Feb%2012%202009%20Memorandum%20of%20US.pdf, [http://perma.cc/9EYZ-D597]. *But see Transcript of President Obama’s Jan. 17 speech on NSA reforms*, *supra* note 11 (suggesting that in the future NSA surveillance will be limited to two hops).

14. SECTION 215 WHITE PAPER, *supra* note 2, at 4.

15. *Id.*

16. *See generally* Memorandum of the United States in Response to the Court’s Order Dated Jan. 28, 2009 at 4 n.3, *In re Prod. of Tangible Things From [REDACTED]*, No. BR 08-13 (FISA Ct. Feb. 17, 2009), available at http://www.dni.gov/files/documents/section/pub_Feb%2012%202009%20Memorandum%20of%20US.pdf, [http://perma.cc/9EYZ-D597] (“Authorizations after this matter was initiated in May 2006 expanded the telephone identifiers that NSA could query to those identifiers associated with [REDACTED] *see generally* docket number BR 06-05 (motion to amend granted in August 2006) . . . docket number BR 07-10 (motion to amend granted in June 2007). The Court’s authorization in docket number BR 08-13 ap-

Since the advent of the program FISC has acknowledged “that the vast majority of the call-detail records provided are expected to concern communications that are (i) between the United States and abroad; or (ii) wholly within the United States, including local telephone calls.”¹⁷ The rationale behind collecting this information is that:

International terrorist organizations and their agents use the international telephone system to communicate with one another between numerous countries all over the world, including to and from the United States. In addition, when they are located inside the United States, terrorist operatives make domestic U.S. telephone calls. The most analytically significant terrorist-related communications are those with one end in the United States or those that are purely domestic, because those communications are particularly likely to identify suspects in the United States—whose activities may include planning attacks against the homeland.¹⁸

The program is thus designed to obtain foreign intelligence and to protect against international terrorist threats both in the United States and overseas. Under the Foreign Intelligence Surveillance Act (FISA), which governs the program, the data obtained is understood as “presumptively relevant to an authorized investigation” where the government can establish that the information pertains to (a) a foreign power or an agent of a foreign power, (b) the activities of a suspected agent of a foreign power who is the subject of such authorized investigation, or (c) an individual in contact with, or known to, a suspected agent of a foreign power who is the subject of an authorized investigation.¹⁹

However important the purpose, the National Security Agency’s bulk collection of telephony metadata embodies precisely what Congress sought to avoid by enacting the 1978 Foreign Intelligence Surveillance Act in the first place. In so doing, the program violates the spirit, as well as the letter, of the law. It also gives rise to troubling constitutional concerns.

proved querying related to [REDACTED] Primary Order, docket number BR 08-13, at 8.”)

17. *Id.* at 2 n.1.

18. SECTION 215 WHITE PAPER, *supra* note 2, at 3.

19. 50 U.S.C. § 1861(b)(2)(A)(i)–(iii) (2006).

Part I of this Article begins by pointing out that the reason Congress introduced FISA was to make use of new technologies and to enable the intelligence community to obtain information vital to U.S. national security, while preventing the NSA and other federal intelligence-gathering entities from engaging in broad domestic surveillance. The legislature sought to prevent a recurrence of the abuses of the 1960s and 1970s that accompanied both the Cold War and the rapid expansion of communications technologies.

Congress accordingly circumscribed the NSA's authorities by limiting them to foreign intelligence gathering. It required that the target be a foreign power or an agent thereof, insisted that such claims be supported by probable cause, and heightened the protections afforded to the domestic collection of U.S. citizens' information. Initially focused on electronic surveillance, FISA expanded over time to incorporate physical searches, pen registers and trap and trace, and searches of business records and tangible goods. The NSA program reflects neither the particularization required by Congress prior to acquisition of information, nor the role Congress anticipated for FISC and the Foreign Intelligence Surveillance Court of Review (FISCR).

The bulk collection program, moreover, as pointed out in Part II of this Article, violates the statutory language in three important ways: (1) it fails to satisfy the requirement that records sought be "relevant to an authorized investigation;" (2) it fails to satisfy the statutory provision that requires that information sought also could be obtained via subpoena duces tecum; and (3) it bypasses the statutory framing for pen registers and trap and trace devices.

Part III of this Article suggests that the bulk collection of U.S. citizens' metadata also gives rise to serious constitutional concerns. Efforts by the government to save the program on grounds of third party doctrine are unpersuasive in light of the unique circumstances of *Smith v. Maryland* and the significant privacy invasions resulting from the universal use of pen registers and trap and trace devices, the evolution of social norms, and the advent of new technologies. In addition, the role of compulsion with regard to the FISC orders (in contrast to the consent of the telephone company in 1979) implicates the Fourth Amendment.

Further examining the Supreme Court's jurisprudence, Part III goes on to note that over the past decade, tension has emerged between the view that new technologies should be considered from the perspective of trespass doctrine and the view that *Katz's* reasonable expectation of privacy test should apply. Cases involving, for instance, GPS chips, thermal scanners, and highly-trained dogs divide along these lines. Regardless of which approach one adopts, however, similar results mark the application of these doctrines to the telephony metadata program.

Under trespass doctrine, the primary order for the program amounts to a general warrant—the elimination of which was the aim of the Fourth Amendment. In light of social norms, it is also a digital trespass on individuals' private spheres.

Under *Katz*, in turn, Americans do not expect that their telephony metadata will be collected and analyzed.²⁰ Most Americans do not even realize what can be learned from such data, making invalid any claim that they reasonably expect the government to have access to such information. The courts also have begun to recognize, in a variety of contexts, the greater incursions into privacy represented by new technologies.

A variant of the government's argument suggests that the mere acquisition of data, absent human intervention, cannot constitute a search. There are multiple problems with this approach, not least of which are that the Supreme Court has never carved out an automation exception; that privacy interests are determined from the perspective of the individual, not the government; and that the decision to collect the information is replete with human interaction. Citations to the usefulness of such information fail to extract the program from a constitutional abyss.

Part IV concludes by calling for an end to the telephony metadata program and the implementation of FISA reforms to enable the government to take advantage of new technologies, to empower the intelligence agencies to respond to national security threats, and to bring surveillance operations within the bounds of statutory and constitutional law. Inserting adversar-

20. *Katz v. United States*, 389 U.S. 347, 360–61 (1967) (Harlan, J., concurring) (finding that the Fourth Amendment protects reasonable expectations of privacy).

ial counsel into the FISA process, creating a repository of technological expertise for FISC and FISCR, restoring prior targeting, heightening protections for U.S. persons, further delimiting relevant data, narrowing the definition of “foreign intelligence” to exclude “foreign affairs,” and requiring the government to demonstrate past effectiveness prior to obtaining renewal orders offer some possibilities for the future of foreign intelligence gathering in the United States.

I. BULK COLLECTION IN THE CONTEXT OF FISA’S GENERAL APPROACH

In the early 1970s, a series of news stories broke detailing the existence of covert domestic surveillance programs directed at U.S. citizens. These revelations led, *inter alia*, to the creation of the Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities. Chaired by Senator Frank Church, the Committee uncovered a range of disconcerting domestic surveillance operations—including some conducted by the NSA—prompting Congress to pass the FISA.

In this legislation, Congress purposefully circumscribed intelligence agencies’ authorities by adopting four key protections.²¹ First, any information obtained from an electronic intercept had to be tied to a specific person or entity, identified as a foreign power or an agent thereof, prior to the collection of the information.²² Second, the government had to demonstrate probable cause that the target, about whom information was to be collected, was a foreign power or an agent thereof.²³ For U.S. persons, probable cause could not be established solely on the basis of otherwise protected First Amendment activities, thus providing U.S. citizens with a higher level of protection.²⁴ Third, Congress adopted minimization procedures to restrict the types of information that could be obtained and retained.²⁵ Fourth, FISA made provision for the Foreign Intelligence Sur-

21. *See* 50 U.S.C. §§ 1801–1811 (1978).

22. *Id.* § 1802(a).

23. *Id.* § 1804(a).

24. *Id.* § 1805(a)(2).

25. *See id.* § 1801(h).

veillance Court to oversee the process.²⁶ Designed to introduce a neutral, disinterested magistrate into the equation, FISC's role was, narrowly, to ascertain whether the government had met the appropriate requirements for targeting *prior* to the acquisition of information. All of these limits dealt, specifically, with electronic communications. Over time, the statute expanded to apply a similar approach to physical searches, the placement of pen registers and trap and trace, and business records—as well as tangible goods.

The telephony metadata program runs contrary to the general approach Congress adopted in FISA both with regard to the particularization otherwise required and the role Congress envisioned for the Foreign Intelligence Surveillance Court and the Court of Review.

A. *Prior Domestic Surveillance*

One of the first public indications that the executive branch was engaging in broad domestic intelligence gathering came in January 1970. Writing in the *Washington Monthly*, Christopher Pyle charged that the Army was engaged in the surveillance of U.S. citizens.²⁷ The following year, an organization calling itself the Citizens' Commission to Investigate the FBI broke into a two-person FBI office in Media, Pennsylvania, stealing 1000 classified documents, all of which *WIN Magazine* subsequently published.²⁸ A code word on these documents, "COINTELPRO" (for "counterintelligence program"), prompted Carl Stern, a reporter for NBC, to initiate a Freedom of Information Act lawsuit.²⁹ On December 6, 1973, Stern

26. *See id.* § 1803.

27. Christopher H. Pyle, *CONUS Intelligence: The Army Watches Civilian Politics*, *WASH. MONTHLY*, Jan. 1, 1970, reprinted in 91 CONG. REC. 2227–2231 (1970).

28. *The Complete Collection of Political Documents Ripped-off from the FBI Office in Media, PA, March 8, 1971*, *WIN MAG.*, Mar. 1972. Note that the original FBI files are now located at the Swarthmore College Peace Collection, Swarthmore College, Swarthmore, Pennsylvania.

29. SELECT COMM. TO STUDY GOV'T OPERATIONS, S. REP. NO. 94-755, SUPPLEMENTARY DETAILED STAFF REPORTS ON INTELLIGENCE ACTIVITIES AND THE RIGHTS OF AMERICANS: FINAL REPORT OF THE SELECT COMMITTEE TO STUDY GOVERNMENTAL OPERATIONS WITH RESPECT TO INTELLIGENCE ACTIVITIES 3 (1976) (citing Letter From FBI Headquarters to All SACs (Apr. 28, 1971), available at <http://archive.org/stream/finalreportofsel03unit#page/n3/mode/2up>,

filed a story that ran on NBC Nightly News, detailing extensive domestic surveillance and disruption undertaken by the FBI for national security purposes.³⁰

In 1974, Seymour M. Hersh, an investigative reporter, published a detailed report in the *New York Times* catapulting the conversation forward. Hersh reported that during the Nixon Administration the Central Intelligence Agency (CIA) had conducted a massive intelligence operation “against the antiwar movement and other dissident groups in the United States.”³¹ A special unit that reported directly to the Director of Central Intelligence had maintained intelligence files on more than 10,000 Americans, including members of Congress.³² The CIA had also engaged in dozens of other illegal operations since the 1950s, such as “break-ins, wiretapping, and the surreptitious inspection of mail.”³³ One official reported that the requirement to keep files on U.S. citizens stemmed, in part, from the so-called Huston plan.³⁴ Agency officials claimed at the time that, although directed at U.S. citizens, everything they had done had been under the auspices of foreign intelligence gathering.³⁵

These new revelations came as quite a surprise, not least because the 1947 National Security Act forbade the Director of the Central Intelligence Agency from having any “police, subpoena, law-enforcement powers or internal-security functions.”³⁶ The report, moreover, came on the heels of a Senate Armed Services Committee report condemning the Pentagon for spying on the White House National Security Council.

[<http://perma.cc/PP98-82PB>]; Memorandum from C.D. Brennan to W.C. Sullivan (Apr. 27, 1971).

30. See Michael Isikoff, *NBC reporter recounts breaking FBI spying story*, NBC NEWS, Jan. 8, 2014, http://investigations.nbcnews.com/_news/2014/01/08/22220561-nbc-reporter-recounts-breaking-fbi-story?lite, [<http://perma.cc/FD5B-3R8K>].

31. Seymour M. Hersh, *Huge C.I.A. Operation Reported in U.S. Against Antiwar Forces, Other Dissidents in Nixon Years*, N.Y. TIMES, Dec. 22, 1974, at 1.

32. *Id.*

33. *Id.*

34. *Id.* at 26. Named for Tom Charles Huston, the Presidential aide who conceived the project, the plan called for the use of burglaries and wiretapping to counter antiwar activities and student turmoil ostensibly “fomented” by black extremists. President Nixon and senior officials claimed that it had never been implemented.

35. *Id.*

36. National Security Act of 1947, Pub. L. No. 253, § 102(d)(3), 61 Stat. 495, 498 (1947).

These public allegations, related to intelligence agencies' impropriety, illegal activities, and abuses of authority, prompted both Houses of Congress to create temporary committees to investigate the accusations: the House Select Committee on Intelligence, and the Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities.³⁷

The latter, Chaired by Senator Frank F. Church (D-ID), with the assistance of Senator John G. Tower (R-TX) as Vice Chairman, was a carefully-constructed, bipartisan initiative. Its membership included eleven Senators, six drawn from the majority party and five from the minority party.³⁸ The Republican leadership in the Senate chose legislators representing a range of views within their party, as did the Democratic leadership.³⁹ Further thought was given to diversity of experience, incorporating both senior members of the Senate as well as some of the most junior members—including one Senator who had only begun his service a few weeks prior to the formation of the committee.⁴⁰ The Senate overwhelmingly supported the establishment of the Select Committee, endorsing its creation by a vote of 82-4.⁴¹

The Senate directed the committee to do two things: first, to investigate “illegal, improper, or unethical activities” in which the intelligence agencies engaged; and, second, to determine the “need for specific legislative authority to govern” the NSA and other agencies.⁴² The Church Committee subsequently took testimony from hundreds of people, inside and outside of government, in public and private hearings. The NSA, FBI, CIA, Internal Revenue Service, Post Office, and other federal agencies submitted documents. In 1975 and 1976 the Committee is-

37. H.R. Res. 138, 94th Cong. (1975), *replaced and expanded* by H.R. Res. 591, 94th Cong. (1975); S. Res. 21, 94th Cong. (1975).

38. *Intelligence Activities: Hearing on S. Res. 21 Before the Select Comm. to Study Governmental Operations with Respect to Intelligence Activities of the United States*, 94th Cong. ii (1975) [hereinafter *Church Committee Report*].

39. Interviews with Senator Walter Mondale and Senator Gary Hart, in Washington, D.C. (Sept. 23, 2013).

40. *Id.*

41. S. Res. 21, 94th Cong., 121 CONG. REC. 1416–34 (1975).

42. *Id.*

sued seven reports and six supplemental volumes, classifying another sixty reports for future release.⁴³

The committee found that broad domestic surveillance programs, conducted under the guise of foreign intelligence collection, had undermined the privacy rights of U.S. citizens.⁴⁴ The NSA figured largely in these concerns.

1. NSA Programs

Although the NSA maintained a definition of foreign intelligence that focused on threats external to the United States, a key contributor to the agency's decision to intercept Americans' communications was the question of whether the definition of foreign communications prevented the acquisition, or merely the analysis, of information not related to foreign intelligence. The NSA adopted—and the Church Committee rejected—the latter approach.

In October 1952, President Truman issued a classified memo that laid out the future of U.S. signals intelligence and created the NSA.⁴⁵ Truman's aims were to (a) strengthen U.S. signals intelligence capabilities, (b) support the country's ability to wage war, and (c) generate information central to the conduct of foreign affairs.⁴⁶ The NSA's mission, accordingly, was to obtain foreign intelligence from foreign electronic communications.⁴⁷

43. Interview with Senator Gary Hart, in Washington, D.C. (Sept. 24, 2013). Since 1992, another 50,000 pages of the records have been declassified and made publicly available at the National Archives. *Rockefeller Commission Report*, HISTORY MATTERS, http://history-matters.com/archive/contents/church/contents_church_reports_rockcomm.htm, [http://perma.cc/0tjNU58CFXR] (last visited March 19, 2014); Press Release, Nat'l Sec. Agency Cent. Sec. Serv., The National Security Agency Releases Over 50,000 Pages of Declassified Documents (June 8, 2011), available at http://www.nsa.gov/public_info/press_room/2011/50000_declassified_docs.shtml, [http://perma.cc/SR2A-TCGK].

44. See *supra* note 38.

45. 5 *Church Committee Report*, *supra* note 38, at 6 (citing Memorandum from President Harry Truman (Oct. 29, 1952)).

46. 5 *Church Committee Report*, *supra* note 38. For an informative discussion of MI-8 and the NSA's predecessor agencies, see House Comm. on Gov't Operations, *Interception of International Telecommunications by the National Security Agency 1-12* (Draft Report), available at <http://www.maryferrell.org/mffweb/archive/viewer/showDoc.do?docId=145022&relPageId=14>, [http://perma.cc/3LK5-CDWR].

47. 5 *Church Committee Report*, *supra* note 38, at 6 (statement of Lieutenant General Lew Allen, Jr., Director, National Security Agency).

From the beginning, the agency understood foreign intelligence to involve the interception of communications wholly or partly outside the United States and not targeted at U.S. persons. Neither the Presidential directive of 1952, nor the National Security Council Intelligence Directive (NSCID) No. 6, which authorized the CIA to engage in Foreign Wireless and Radio Monitoring, defined the term “foreign communications.”⁴⁸

NSCID No. 9, however, titled “Communications Intelligence,” defined “foreign communications” as “all telecommunications and related materials . . . of the government and/or their nationals or of any military, air, or naval force, faction, party, department, agency, or bureau of a foreign country, or of any person or persons acting or purporting to act therefor.” It included “all other telecommunications and related material of, to, and from a foreign country which may contain information of military, political, scientific or economic value.”⁴⁹ “Foreign communications” thus turned upon the nature of the entity engaged in communications: a foreign power, or an individual acting on behalf of a foreign power.

The NSA did not (indeed, could not) discuss NSCID No. 9 during the Church Committee’s public hearings. The Director of Central Intelligence, however, had issued a directive that the NSA did discuss, which employed a definition of foreign communications that *excluded* communications between U.S. citizens or entities.⁵⁰ In keeping with these understandings, the NSA ostensibly focused on communications conducted wholly or partly outside the United States and not targeted at U.S. persons. The distinction was drawn, however, at the point of analysis—not the point of interception.

Testifying in 1975, NSA Director Lieutenant General Lew Allen, Jr. could thus assert that the NSA did not at that time, nor had it (with one exception—individuals whose names were

48. National Security Council Intelligence Directive No. 6 (Dec. 12, 1947) (National Archives and Records Administration, RG 59, Records of the Department of State, Records of the Executive Secretariat, NSC Files: Lot 66 D 148, Dulles-Jackson-Correa Report, Annex 12); see also 5 *Church Committee Report*, *supra* note 38, at 6.

49. National Security Council Intelligence Directive No. 9 (Mar. 10, 1950) (on file at National Archives and Records Administration, RG 59, Records of the Department of State, Records of the Executive Secretariat, NSC Files: Lot 66 D 195).

50. 5 *Church Committee Report*, *supra* note 38, at 9.

contained on the NSA's watch list) "conducted intercept operations for the purpose of obtaining the communications of U.S. citizens."⁵¹ Whether such communications were incidentally intercepted, however, was another matter. As Lieutenant General Allen recognized, "[S]ome circuits which are known to carry foreign communications necessary for foreign intelligence will also carry personal communications between U.S. citizens, one of whom is at a foreign location."⁵²

Central to Allen's assertion was the understanding that, to constitute foreign communications, and to legitimate the collection of information on U.S. citizens, the target of the surveillance must be a foreign power, or an agent of a foreign power, and at least one party to each communication must be outside the country.

The Senate considered this approach, in light of the broad swathes of information obtained about U.S. citizens, to run afoul of the Fourth Amendment. Two NSA programs in particular generated significant concern. The first, Project MINARET, introduced to collect foreign intelligence information, ended up intercepting hundreds of U.S. citizens' communications. The second, Operation SHAMROCK, involved the large-scale collection of U.S. citizens' communications from private companies.

a. Project MINARET

In the late 1960s, the NSA, like the Internal Revenue Service (IRS), the FBI, and the CIA, constructed a list of U.S. citizens and non-U.S. citizens subject to surveillance.⁵³ The program, which operated from 1967 to 1973 started out by narrowly focusing on the international communications of U.S. citizens traveling to Cuba. It quickly expanded, however, to include individuals (a) involved in civil disturbances, (b) suspected of criminal activity, (c) implicated in drug activity, (d) of concern to those tasked with Presidential protection, and (e) suspected of involvement in international terrorism.⁵⁴

51. *Id.*

52. *Id.*

53. *Id.* at 3.

54. *Id.* at 10-11.

In 1969 the collection of information on individuals included on the watch list became known as Project MINARET.⁵⁵ When details about the program emerged, senators and members of the public expressed alarm about the privacy implications. Central to the legislators' concern was the potential for such programs to target communications of a wholly domestic nature. Senator (later Vice President) Walter Mondale articulated the Committee's disquiet:

Given another day and another President, another perceived risk and someone breathing hot down the neck of the military leader then in charge of the NSA: demanding a review based on another watch list, another wide sweep to determine whether some of the domestic dissent is really foreign based, my concern is whether that pressure could be resisted on the basis of the law or not [W]hat we have to deal with is whether this incredibly powerful and impressive institution . . . could be used by President 'A' in the future to spy upon the American people [W]e need to . . . very carefully define the law, spell it out so that it is clear what [the Director of the NSA's] authority is and . . . is not.⁵⁶

Senator Mondale asked Allen whether he would object to a new law clarifying that the NSA did *not* have the authority to collect domestic information on U.S. citizens. Allen indicated that he did not object.⁵⁷ FISA subsequently became the instrument designed to limit the NSA's collection of information on U.S. citizens.

b. Operation SHAMROCK

During the Senate hearings, much concern was expressed about whether to make public a second, highly classified, large-scale surveillance program run by the NSA.⁵⁸ The committee decided to discuss the program in open session on the grounds that it was both illegal and violated the Fourth Amendment.⁵⁹

55. *Id.* at 30.

56. *Id.* at 36.

57. *Id.*

58. *Id.* at 48–57, 60–61, 63; *see also* House Comm. on Gov't Operations, *supra* note 46, at 2–6 (discussing pressures on the Church Committee from the House side).

59. 5 *Church Committee Report*, *supra* note 38, at 57 (statement of Senator Frank Church, Chairman, Select Comm. to Study Governmental Operations with Respect to Intelligence Activities of the United States Senate).

Operation SHAMROCK was the cover name given to a program in which the government had convinced three major telegraph companies (RCA Global, ITT World Communications, and Western Union International) to forward international telegraphic traffic to the Department of Defense.⁶⁰ For nearly thirty years, the NSA and its predecessors received copies of most international telegrams that had originated in, or been forwarded through, the United States.⁶¹

Operation SHAMROCK stemmed from wartime measures, in which companies turned messages related to foreign intelligence targets over to military intelligence. In 1947, the Department of Defense negotiated the continuation of the program in return for protecting the companies from criminal liability and public exposure.⁶²

Like Project MINARET, the scope of the program gradually expanded. Initially, the program focused on foreign targets. Eventually, however, as new technologies became available, the NSA began extracting U.S. citizens' communications.⁶³ It selected approximately 150,000 messages per month for further analysis, distributing some messages to other agencies.⁶⁴

Senators expressed strong concern at the resulting privacy violations, inviting the Attorney General before the Select Committee to discuss "the fourth amendment of the Constitution and its application to 20th century problems of intelligence and surveillance."⁶⁵ Senator Frank Church explained:

In the case of the NSA, which is of particular concern to us today, the rapid development of technology in the area of electronic surveillance has seriously aggravated present ambiguities in the law. The broad sweep of communications interception by NSA takes us far beyond the previous fourth amendment controversies where particular individuals and specific telephone lines were the target.⁶⁶

60. *Id.* at 57–58.

61. *Id.* at 58.

62. *Id.*

63. *Id.* at 58–59.

64. *Id.* at 60.

65. *Id.* at 65.

66. *Id.*

Lieutenant General Allen sought to reassure the committee that although some circuits carried personal communications, the interception was “conducted in such a manner as to minimize the unwanted messages.”⁶⁷ Nevertheless, the agency could have obtained many unwanted communications, and thus undertook procedures to process, sort, and analyze the relevant data. “The analysis and reporting is accomplished only for those messages which meet specified conditions and requirements for foreign intelligence.”⁶⁸ Elaborating further, Allen noted, “[t]he use of lists of words, including individual names, subjects, locations, etc., has long been one of the methods used to sort out information of foreign intelligence value from that which is not of interest.”⁶⁹

The question that confronted Congress was how to limit the NSA’s ability to acquire broad swathes of information up front, in the process obtaining access to private communications of individuals with no connection to foreign intelligence concerns. Congress would have to find a way to control new, sophisticated technologies and to allow intelligence agencies to perform their legitimate foreign intelligence activities, without also allowing the agencies to invade U.S. citizens’ privacy by allowing them access to information unrelated to national security.⁷⁰

In the absence of any governing statute, Attorney General Edward H. Levi’s approach had been to authorize the requested surveillance only where a clear nexus existed between the target and a foreign power.⁷¹ The Attorney General sought to distinguish the process from the British Crown’s use of writs of assistance, in the shadow of which James Madison had drafted the Fourth Amendment.⁷² The Founders’ objection to such instruments was simple: Were the government to be granted the

67. *Id.* at 19.

68. *Id.* Former CIA Director William E. Colby provided similar testimony before the Pike Committee on August 6, 1975: “On some occasions, [the interception of U.S. citizens’ communications] cannot be separated from the traffic that is being monitored. It is technologically impossible to separate them.” *U.S. Intelligence Agencies and Activities: Intelligence Costs and Fiscal Procedures: Hearings Before the H. Select Comm. on Intelligence*, 94th Cong. 241 (1975) (statement of William E. Colby, Acting Director, CIA).

69. 5 *Church Committee Report*, *supra* note 38, at 20.

70. *Id.*

71. *Id.* at 71.

72. *Id.* at 71–72.

authority to break into and search individuals' homes without cause, the private affairs of every person would be subject to inspection.⁷³ In contrast, Levi argued, the exercise of electronic wiretaps for foreign intelligence gathering fell subject to Attorney General review. Nevertheless, he recognized the need for new laws to address the ambiguity that attended the use of modern technologies. The senators agreed.⁷⁴

2. Broader Context

The NSA was not the only federal entity making use of new technologies to collect significant amounts of information on U.S. citizens. The FBI, CIA, IRS, U.S. Army, and other federal entities similarly engaged in broad domestic intelligence-gathering operations. Details relating to many of these programs, such as the FBI's COINTELPRO and the CIA's Operation CHAOS, were uncovered by the exhaustive investigations of the Senate Select Committee and other entities that looked into the range and extent of programs underway.⁷⁵ Both statutory violations and constitutional concerns accompanied these inquiries.

In 1970, for instance, Senator Sam Ervin (D-NC) began investigating the public allegations. After a year of making minimal progress in the face of misleading statements from the Nixon Administration, claims of inherent executive power, and a refusal to disclose information that might damage national security, Senator Ervin called for public hearings to consider "the dangers which the Army's program presents to the principles of the Constitution."⁷⁶

In 1975, President Ford issued an executive order establishing the President's Commission on CIA Activities Within the United States (the "Rockefeller Commission").⁷⁷ Ford appointed Vice President Nelson Rockefeller as chairman.⁷⁸ The public charges to which the Rockefeller Commission responded included large-scale domestic surveillance of U.S. citizens, retain-

73. *Id.* at 72.

74. *See, e.g., id.* at 64–65, 84, 125.

75. *See, e.g., id.* at 3.

76. 116 CONG. REC. 26,329 (1970).

77. *See* Exec. Order No. 11,828, 3 C.F.R. 933 (1975).

78. Commission on CIA Activities Within the United States: Announcement of Appointment of Chairman and Members, 11 WEEKLY COMP. PRES. DOC. 25 (Jan. 5, 1975).

ing dossiers on U.S. citizens, and aiming these activities at individuals who disagreed with government policies.⁷⁹ The Commission's aim was further supplemented by allegations that the CIA had intercepted and opened personal mail in the United States for the past twenty years, infiltrated domestic dissident groups and intervened in domestic politics, engaged in illegal wiretaps and break-ins, and improperly assisted other government agencies.⁸⁰

Like the Senate Select Committee, the Rockefeller Commission faced the key question of how to define the term "foreign intelligence"—a crucial step in protecting Americans' right to privacy. Accordingly, in its first recommendation, the Rockefeller Commission advised that Section 403 of the 1947 National Security Act be amended to make it explicit that the CIA's activities must be solely related to "foreign intelligence."⁸¹ Any involvement of U.S. citizens could only be incidental to foreign intelligence collection.⁸²

The Commission reinforced the strict separation between foreign targets and U.S. persons through its second recommendation: that the President, by executive order, "prohibit the CIA from the collection of information about the domestic activities of United States citizens (whether by overt or covert means), the evaluation, correlation, and dissemination of analyses or reports about such activities, and the storage of such information."⁸³

The House Select Intelligence Committee, created on February 19, 1975, was replaced five months later by a committee headed by Representative Otis Pike (D-NY).⁸⁴ The Pike Committee focused on a range of intelligence gathering programs, including those of the National Security Agency.⁸⁵ Public hear-

79. REPORT TO THE PRESIDENT BY THE COMMISSION ON CIA ACTIVITIES WITHIN THE UNITED STATES 9 (1975).

80. *Id.*

81. *Id.* at 12.

82. *Id.* at 12–13.

83. *Id.* at 13.

84. H.R. Res. 138, 94th Cong. (Feb. 19, 1975) (introduced Jan. 16, 1975 and passed Feb. 19, 1975 by a vote of 286–120).

85. See, e.g., 1 *U.S. Intelligence Agencies and Activities: Intelligence Costs and Fiscal Procedures: Hearings Before the H. Select Comm. on Intelligence*, 94th Cong. (1975); 3 *U.S. Intelligence Agencies and Activities: Domestic Intelligence Programs: Hearings Before the H. Select Comm. on Intelligence*, 94th Cong. (1975); 4 *U.S. Intelligence Agen-*

ings on the agency's operations were held in October 1975 and February and March 1976.⁸⁶ Its draft report complained of the tension between Congress and the executive branch, noting the "intense Executive branch efforts" to have the NSA hearings curtailed or postponed—both in the Senate and the House.⁸⁷

Like the Church Committee, the Pike Committee expressed concern about SHAMROCK and MINARET, noting that the former resulted in the NSA maintaining files on approximately 75,000 U.S. citizens between 1952 and 1974:

Persons included in these files included civil rights leaders, antiwar activists, and Members of Congress. For at least 13 years, CIA employees were given unrestricted access to these files, and one or more worked full time retrieving information that presumably was contributed to the CIA's domestic intelligence program—Operation CHAOS—which existed from 1967 to 1974.⁸⁸

For the Pike Committee, these programs violated both Section 605 of the Communications Act and the Fourth Amendment.⁸⁹

The committee expressed particular concern about the NSA's "vacuum cleaner" approach to foreign intelligence gathering.⁹⁰ The committee noted that international telephone calls, some twenty-four million telegrams and fifty million telex (teletype) messages entered, left, and transited the United States each year, and millions of additional messages that traveled over leased lines—"including millions of computer data transmissions electronically entering and leaving the country"—presented further potential sources of intelligence.⁹¹

Coming on the heels of the Pentagon Papers, which demonstrated that the Johnson Administration had systematically lied to the public and to Congress; the Watergate scandal, in which the Nixon Administration orchestrated a June 1972 break-in at the Democratic National Committee headquarters; and Presi-

cies and Activities: Committee Proceedings: Proceedings of the H. Select Committee on Intelligence, 94th Cong. (1975).

86. House Comm. on Gov't Operations, *supra* note 46, at 2.

87. *Id.*

88. *Id.* at 14.

89. *Id.* at 15–17.

90. *Id.* at 18.

91. *Id.*

dent Nixon's resignation on August 9, 1974, the revelation of these programs deepened the erosion of public confidence in the executive branch. More specifically, their findings undermined citizens' confidence in the intelligence agencies.⁹² Critical questions facing Congress were how to rebuild confidence in the system, how to incorporate new technologies into the existing infrastructure, and how to empower the intelligence agencies to conduct electronic surveillance, while protecting the privacy rights of U.S. citizens.

A timely judicial decision helped to lay the groundwork for congressional action. In 1972 the Supreme Court had held that the electronic surveillance of domestic groups, even where security issues might be involved, required that the government first obtain a warrant.⁹³ The "inherent vagueness of the domestic security concept," and the significant possibility that it could be abused to quash political dissent, underscored the importance of the Fourth Amendment—particularly when the government was spying on its own citizens.⁹⁴

Justice Powell, writing for the Court, emphasized the limits of the decision: "[T]his case involves only the domestic aspects of national security. We have not addressed, and express no opinion as to, the issues which may be involved with respect to activities of foreign powers or their agents."⁹⁵ Standards and procedures for domestic security surveillance might differ from those required by Title III of the Omnibus Crime Control and Safe Streets Act of 1968.⁹⁶ Congress may wish to consider passing new laws covering such cases.⁹⁷

Four critical changes followed. First, consistent with the Church Committee's recommendations, Congress created a permanent Senate Intelligence Committee. Within a month of the final report, a resolution to this effect was introduced, and on May 19, 1976 it passed by overwhelming majority, 72-22.⁹⁸ The new Senate Select Committee on Intelligence (SSCI) was

92. 124 CONG. REC. 36,415 (1978) (statement of Rep. Morgan Murphy).

93. *United States v. U.S. District Court*, 407 U.S. 297 (1972).

94. *Id.* at 320.

95. *Id.* at 321-22.

96. *See id.* at 322.

97. *See id.* at 322-23.

98. S. Res. 400, 94th Cong. (1976).

given exclusive oversight of the CIA and concurrent jurisdiction over the NSA and other elements of the intelligence community.⁹⁹ The resolution directed that the intelligence community keep the new entity “fully and currently informed” of their activities, including all “significant anticipated activities.”¹⁰⁰ It was to be a “select,” rather than a “standing,” committee, precisely to allow the Senate majority and minority leaders to decide its composition, and to avoid the same in the party caucuses preceding each new Congress.¹⁰¹ The chair and vice chair would not be allowed to serve concurrently as chair or ranking minority member of any major standing committee.¹⁰²

Of the fifteen members selected, no more than eight would be drawn from the majority party, ensuring balance between the parties.¹⁰³ In addition, the Committee’s composition would ensure cross-representation of related committees: Two members each would be drawn from the Appropriations, Armed Services, Foreign Relations, and Judiciary Committees.¹⁰⁴ A limit of eight years was placed on committee membership, to avoid intelligence agency capture.¹⁰⁵ Notably, five of the first fifteen members, Walter Huddleston (D-KY), Gary Hart (D-CO), Robert Morgan (D-NC), Barry Goldwater (R-AZ), and Howard Baker (R-TN), had served as members of the Church Committee. Fourteen members of SSCI’s staff had served as staff members to the same, including William Miller, the staff director for both the Church Committee and the newly-minted SSCI.¹⁰⁶

99. *Id.*

100. *Id.*

101. *Id.*

102. *Id.*

103. *Id.*

104. *Id.*

105. *Id.*

106. Interview with William Miller, in Washington, D.C. (Sept. 24, 2013). For discussion of the history of the founding of this committee and its subsequent development, see SENATE SELECT COMM. ON INTELLIGENCE, LEGISLATIVE OVERSIGHT OF INTELLIGENCE ACTIVITIES: THE U.S. EXPERIENCE, S. DOC. NO. 82-692 (1994). See also FRANK J. SMIST, JR., CONGRESS OVERSEES THE UNITED STATES INTELLIGENCE COMMUNITY, 1947-1989 (1990); L. BRITT SNIDER, THE AGENCY AND THE HILL: CIA’S RELATIONSHIP WITH CONGRESS, 1946-2004, 51-91 (2008). Following the rather dismal mood that marked the Pike Committee’s operations, the House Permanent Select Committee on Intelligence was not founded until July 17, 1977. At that point, House Resolution 658 passed 227-171, creating the Permanent Select Committee on Intelli-

Second, the President issued an executive order “to improve the quality of intelligence needed for national security, to clarify the authority and responsibilities of the intelligence departments and agencies, and to establish effective oversight to assure compliance with law in the management and direction of intelligence agencies and departments of the national government.”¹⁰⁷

Executive Order 11,905 prohibited the CIA from engaging in electronic surveillance in the United States and banned intelligence agencies from engaging in physical surveillance, electronic surveillance, unconsented physical searches, mail opening, or examining federal tax returns except as consistent with procedures approved by the Attorney General or in accordance with applicable statutes and regulations.¹⁰⁸ It prohibited the infiltration of organizations for the purpose of reporting on their activities, with the exception of organizations primarily composed of non-U.S. persons that were reasonably believed to be acting on behalf of a foreign power.¹⁰⁹ The order further prevented any *collection* of information about U.S. persons’ domestic activities absent situations with a clear foreign intelligence or counterintelligence component.¹¹⁰

Despite the provisions contained in the executive order, Congress considered legislative action crucial to reining in the intelligence agencies and therefore, as a third outcome, chose to rewrite the National Security Act to require a finding and notification for covert action.

gence (HPSCI). The structure of both committees remained relatively constant until 2004. The National Commission on Terrorist Attacks upon the United States issued its report in July 2004, criticizing the system of congressional oversight of intelligence agencies as “dysfunctional” and recommending either a joint committee on intelligence (similar to the Joint Atomic Energy Committee), with authority both to authorize and appropriate, or smaller committees, and the elimination of term limits. U.S. NAT’L COMM’N ON TERRORIST ATTACKS UPON THE UNITED STATES, THE 9/11 COMMISSION REPORT: FINAL REPORT 420–21 (2004). In 2004, the Senate eliminated the eight-year term limits, elevated the committee to category A (Senators are generally only able to serve on up to two “A” Committees), created an oversight subcommittee, and created an intelligence subcommittee in the Appropriations Committee. S. Res. 445, 108th Cong. (2004).

107. Exec. Order No. 11,905, 41 Fed. Reg. 7703 (Feb. 19, 1976). This order was subsequently strengthened by Exec. Order No. 12,036, 43 Fed. Reg. 3674 (Jan. 26, 1978), and replaced in part by Exec. Order No. 12,333, 46 Fed. Reg. 59,941 (Dec. 8, 1981).

108. Exec. Order No. 11,905, § 5(b)(1)–(5), 41 Fed. Reg. at 7728–30.

109. *Id.* § 5(b)(6).

110. *Id.* § 5(b)(7).

Fourth, Congress passed the Foreign Intelligence Surveillance Act. The aim was to empower the intelligence agencies to collect information necessary to protect U.S. national security, while preventing agencies from using foreign intelligence gathering as an excuse for engaging in domestic surveillance of U.S. citizens. The process began with the Foreign Intelligence Surveillance Act of 1976, the first bill introduced in Congress, which was supported by the President and Attorney General and would require judicial warrants in foreign intelligence cases.¹¹¹ Its successor bill, S. 1566, became the Foreign Intelligence Surveillance Act of 1978.¹¹²

B. Protections Built into FISA

From the beginning, Congress made it clear that the legislation was designed to prevent precisely the types of broad surveillance programs and incursions into privacy represented by Project MINARET, Operation SHAMROCK, COINTELPRO, Operation CHAOS, and other intelligence-gathering initiatives that had come to light.¹¹³ During consideration of the conference report on S. 1566, for instance, Senator Ted Kennedy (D-MA) noted, “The abuses of recent history sanctioned in the name of national securi-

111. 124 CONG. REC. 35,389 (1978) (statement of Sen. Charles Matthias, Jr.); *see also* Foreign Intelligence Surveillance Act of 1976, S. 3197, 94th Cong. (1976).

112. *See* Pub. L. No. 95-511, 92 Stat. 1783; 124 CONG. REC. 35,389 (1978).

113. Proponents of the bulk metadata collection program assert that the statute was not intended to protect against invasive surveillance. Instead, the statute “creates a balance between the criminal system’s restrictions on government searches and the broader acceptance of information-gathering during wartime.” John Yoo, *The Legality of the National Security Agency’s Bulk Data Surveillance Programs*, 37 HARV. J.L. PUB. POL’Y 901, 906 (2014). There are three problems with this claim. First, the two statements are not in opposition—that is, the program could be oriented toward curbing government surveillance even as it seeks a balance between competing concerns. Second, the historical record does not support the first part of the claim. The entire *raison d’être* behind FISA was to create a framework to protect against overzealous use of surveillance. Third, FISA does not balance wartime information gathering with criminal law standards. It creates a framework for national security, regardless of whether the country is engaged in hostilities. The legislation specifically contemplates war, creating a short period of suspension, following which the FISA procedures must again be followed. Instead of a “wartime information gathering scheme[]”, it would be more accurate to describe FISA as establishing a national security framework that applies regardless of whether or not the country is at war. *See id.*

ty highlighted the need for this legislation.”¹¹⁴ For Kennedy, the legislation represented the “final chapter in the ongoing 10-year debate to regulate foreign intelligence electronic surveillance.”¹¹⁵ With the passage of FISA, the Senate would “at long last place foreign intelligence electronic surveillance under the rule of law.”¹¹⁶ Senator Birch Bayh, Jr. (D-IN) echoed Kennedy’s sentiments: “This bill, for the first time in history, protects the rights of individuals from government activities in the foreign intelligence area.”¹¹⁷ Senator Charles Mathias (R-MD) noted that enactment of the legislation would be a milestone, ensuring “that electronic surveillance in foreign intelligence cases will be conducted in conformity with the principles set forth in the fourth amendment.”¹¹⁸

The Foreign Intelligence Act of 1978 represented the culmination of a multi-branch, multi-year, cross-party initiative directed at bringing the collection of foreign intelligence within a narrowly circumscribed legal framework.¹¹⁹ Congress consulted the NSA, FBI, CIA, and representatives of interested citizen groups, gaining broad support for the measure.¹²⁰ As a result, FISA passed by significant majorities.¹²¹

Congress purposefully circumscribed the NSA’s authorities in the Foreign Intelligence Surveillance Act by adopting four key protections. First, any information obtained from an electronic intercept had to be tied to a specific person or entity, identified

114. 124 CONG. REC. 34,845 (1978).

115. *Id.*

116. *Id.*

117. *Id.*

118. 124 CONG. REC. 35,389 (1978) (statement of Senator Mathias).

119. In 1972, the Senate Committee on the Judiciary’s Subcommittee on Administrative Practice and Procedure held extensive hearings on the subject of warrantless wiretapping. 122 CONG. REC. 7543 (1976). In 1975, the subcommittee issued a report jointly with a special subcommittee of the Foreign Relations Committee, calling for Congress to introduce legislation governing foreign intelligence collection. *Id.* In 1976, President Ford and Attorney General Levi introduced the Foreign Intelligence Surveillance Act of 1976, H.R. 12,750, 94th Cong. (as introduced in the House, Mar. 23, 1976). President Carter and Attorney General Bell subsequently supported S. 1566, which became FISA. 124 CONG. REC. 36,409 (1978).

120. 124 CONG. REC. 37,738 (1978); 124 CONG. REC. 36,414 (1978).

121. S. 1566 passed the Senate 95-1. 124 CONG. REC. 36,409 (1978). H.R. 7308 passed the House 246-128. *Id.* In October 1978, the Senate adopted the Conference Report “by an overwhelming voice vote, with no dissenting voice vote.” *Id.* The House, in turn, adopted the Conference Report by a vote of 226-176. 124 CONG. REC. 36,417-18 (1978).

as a foreign power or an agent thereof, *before the collection* of the information.¹²² Second, the government had to demonstrate probable cause that the target, about whom information was to be collected, was a foreign power or an agent thereof.¹²³ For U.S. persons, such probable cause could not be established solely on the basis of otherwise protected First Amendment activities, thus providing U.S. citizens with a higher level of protection.¹²⁴ Third, Congress adopted minimization procedures to restrict the type of information that could be obtained and retained.¹²⁵ Fourth, FISA provided for a Foreign Intelligence Surveillance Court (FISC) to oversee the process.¹²⁶ Designed to introduce a disinterested magistrate into the equation, FISC's role was, narrowly, to ascertain whether the government had met the appropriate requirements for targeting *before* the acquisition of information. All of these restrictions centered on the interception of electronic communications. Over time, the statute expanded to apply a similar approach to physical searches, the placement of pen registers and trap and trace, and searches of business records, as well as tangible goods.

1. *Entity Targeted Prior to Acquisition*

From the outset, Congress sought to limit the amount of information the NSC and others acquired by requiring that the target of surveillance be identified as a foreign power or an agent of a foreign power *prior* to the interception of communications. FISA defined a "foreign power" as:

- (1) a foreign government or any component thereof, whether or not recognized by the United States;
- (2) a faction of a foreign nation or nations, not substantially composed of United States persons;
- (3) an entity that is openly acknowledged by a foreign government or governments to be directed and controlled by such foreign government or governments;

122. 50 U.S.C. § 1802(a) (2006).

123. *Id.* § 1804(a).

124. *Id.* § 1805(a)(2).

125. *Id.* § 1801(a).

126. *Id.* § 1803.

- (4) a group engaged in international terrorism or activities in preparation therefor;
- (5) a foreign-based political organization, not substantially composed of United States persons; or
- (6) an entity that is directed and controlled by a foreign government or governments.¹²⁷

Before passage of the bill, the Senate defined “foreign power,” with regard to terrorist groups, to mean a foreign-based entity. The House amendments, in contrast, understood “foreign power” to include groups engaged in international terrorism or activities in preparation therefor. In the end, the Conference adopted the House definition, with the idea that limiting such surveillance solely to foreign-based groups would be “unnecessarily burdensome.”¹²⁸

Throughout the nuanced discussion of the definition of “foreign power” in both houses was the understanding that *prior* to collection of information, the government would have to establish that the target—in relation to which such information would be obtained—qualified as a foreign power or an agent thereof.¹²⁹

In focusing on the targets of the communications, Congress rejected the NSA’s previous (and current) reading of what constituted a “target” in relation to data collection.¹³⁰ That is, the information to be obtained, *at the moment of acquisition* (not in the context of subsequent analysis—the position Lieutenant General Allen advocated for during the Church Committee hearings, which the NSA has recently resurrected), had to relate directly to the individual or entity believed to be a foreign power or an agent thereof.

127. *Id.* § 1801(a).

128. 124 CONG. REC. 33,782 (1978); *see also* 50 U.S.C. § 1801.

129. 124 CONG. REC. 33,784 (1978).

130. 5 *Church Committee Report*, *supra* note 38, at 16 (testimony of Lieutenant General Lew Allen, Jr.); Daniel F. Gilmore, *Director Emphatic: NSA Does Not Bug Americans*, WASH. POST, July 23, 1977, at A2 (“There are no U.S. citizens now targeted by NSA in the United States or abroad.” (quoting Statement of Bobby R. Inman, Director, NSA, Before the Senate Subcommittee on Intelligence and Human Rights)).

2. *Probable Cause and Showing of Criminal Wrongdoing
Prior to Collection*

A second protection stemmed from concerns evinced in the Senate about how to determine whether the (specific) target was a “foreign power” or “an agent thereof.” Foremost in legislators’ minds was the need to provide heightened protections for surveillance targets generally and U.S. citizens in particular. The final bill accomplished this in two ways: by adopting of a standard of probable cause and, under certain circumstances, requiring a showing of criminal wrongdoing in order to acquire information. These elements underscore the particularity Congress required before foreign intelligence gathering was allowed.

FISA incorporated a standard of probable cause.¹³¹ Unlike criminal law—in which the courts required establishing probable cause that a target had committed, was committing, or was about to commit a particular offense—under FISA, the agency requesting surveillance had to demonstrate probable cause that the entity to be placed under surveillance was a “foreign power” or “an agent thereof,” and that the target was likely to use the facilities to be monitored.¹³² For some entities, FISA also required a criminal showing for that entity to be considered a “foreign power.”¹³³ Foreign governments are excluded from this rule. When they are directly involved, no showing of crim-

131. 50 U.S.C. § 1805(a)(3).

132. Compare 18 U.S.C. § 2518(3)(a) (2006) (requiring, under Title III, that the court must find “on the basis of the facts submitted by the applicant that . . . there is probable cause for belief that an individual is committing, has committed, or is about to commit a particular offense enumerated in section 2516 of this chapter”), with 50 U.S.C. § 1805(a)(3) (requiring, in contrast, that FISC find “on the basis of the facts submitted by the applicant,” that “there is probable cause to believe that . . . the target of the electronic surveillance is a foreign power or an agent of a foreign power: *Provided*, That no United States person may be considered a foreign power or an agent of a foreign power solely upon the basis of activities protected by the first amendment to the Constitution of the United States.”). Note that for ordinary criminal law regarding wire and oral communications (for example, telephone and microphone interceptions), section 2516 enumerates predicate offenses that qualify, such as bank fraud (18 U.S.C. § 1344) unlawful possession of a firearm (18 U.S.C. § 922(g)) espionage (for example, 18 U.S.C. § 794), assassination (for example, 18 U.S.C. §§ 351, 1751), sabotage (for example, 18 U.S.C. § 2155), and terrorism (for example, 18 U.S.C. § 2332). For electronic communications (for example, e-mail), any federal felony may serve as a predicate. 18 U.S.C. § 2516(3).

133. See, e.g., 50 U.S.C. § 1801(c)(1).

inal activity is required. Any foreign government, regardless of whether it is an ally or an enemy of the United States, is designated a “foreign power.”¹³⁴

For groups to qualify as foreign powers because they are engaged in international terrorism,¹³⁵ they must be involved in criminal activity. The statute defines “international terrorism” to include, *inter alia*, “activities that . . . involve violent acts or acts dangerous to human life that are a violation of the criminal laws of the United States or of any State, or that would be a criminal violation if committed within the jurisdiction of the United States or any State.”¹³⁶ Acts that would qualify individuals for inclusion in this category must be acts that would be criminal if committed within the United States.

A group may be a “foreign power” not only when it engages in international terrorism, but also when engaged in “activities in preparation therefor.”¹³⁷ This may or may not exceed the criminal “attempt” standard, which is broadly understood as requiring a “substantial step” toward the completion of an offense.¹³⁸ Nevertheless, a “group” engaged in preparatory activities for international terrorism would satisfy criminal conspiracy standards.¹³⁹

For agents of a foreign power, Congress inserted heightened protections for U.S. persons.¹⁴⁰ Specifically, FISA defines “agent of a foreign power” as:

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

134. *Id.* § 1801(a)(1).

135. *Id.* § 1801(a)(4).

136. *Id.* § 1801(c).

137. *Id.* § 1801(a)(4).

138. *Braxton v. United States*, 500 U.S. 344, 349 (1991). This is not broader, however, than the “overt act” requirement contained in some criminal conspiracy statutes. *See, e.g.*, 18 U.S.C. § 371; *see also* Supplemental Brief for the United States app., *In re Sealed Case*, 310 F.3d 717 (FISA Ct. Rev. 2002) (No. 02-001) (comparing FISA and Title III), *available at* <https://www.fas.org/irp/agency/doj/fisa/092502sup.html>, [<http://perma.cc/68JX-BR3N>].

139. 18 U.S.C. § 371.

140. A “United States person” is understood under the statute as “a citizen of the United States, an alien lawfully admitted for permanent residence (as defined in section 1101(a)(20) of title 8), an unincorporated association a substantial number of members of which are citizens of the United States or aliens lawfully admitted for permanent residence, or a corporation which is incorporated in the United States, but does not include a corporation or an association which is a foreign power, as defined in subsection (a)(1), (2), or (3) of this section.” 50 U.S.C. § 1801(i).

- (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) of this section;
 - (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 statutes 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;
 - (D) knowingly enters the United States under a false or fraudulent identity for or on behalf of a foreign power or, while in the United States, knowingly assumes a false or fraudulent identity for or on behalf of a foreign power; or
 - (E) 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).¹⁴¹

141. 50 U.S.C. § 1801(b).

These rules stipulate that U.S. persons may be considered agents of a foreign power only if their actions are consistent with the five provisions in the second section. Taken together, three categories emerge under which a U.S. person can be considered “an agent of a foreign power”: the person (1) engages in espionage and clandestine intelligence activities; (2) engages in sabotage and international terrorism (or aids, abets, or conspires to do the same); or (3) enters the United States under a false identity. This means that for U.S. persons, for the most part, evidence of criminality on par with criminal law must be established before the collection of information.

Looking more closely, the first category requires that the individual knowingly engage in espionage and clandestine intelligence activities. Unlike the other two categories, there is some variation here from criminal law, specifically with regard to the “may involve” standard of Section 1801(b)(2)(A).¹⁴² Something less than the showing of probable cause required in ordinary criminal cases would satisfy this provision. Thus, for counterintelligence operations, something less than probable cause is required for evidence of criminality. But for a U.S. person to fall into this category, some evidence of criminality must be involved.

For the second category, sabotage and international terrorism, the term “sabotage” is defined as “activities that involve a violation of chapter 105 of title 18, or that would involve such a violation if committed against the United States.”¹⁴³ “International terrorism,” in turn, as noted above, is also defined in terms of activities that are criminal or would be criminal if the United States were directly involved. To be considered “an agent of a foreign power” (and thus subject to surveillance under FISA), a U.S. person must actually be engaged in such activities, or activities in preparation for sabotage or international terrorism—or knowingly aiding, abetting, or conspiring with others engaged in similar activities.¹⁴⁴

142. *Id.* § 1801(b)(2)(A).

143. *Id.* § 1801(d).

144. *Id.* § 1801(b)(2)(E).

These provisions reflect criminal law standards.¹⁴⁵ As the House of Representatives explained in the introduction to FISA:

This standard requires the Government to establish probable cause that the prospective target knows both that the person with whom he is conspiring or whom he is aiding or abetting is engaged in the described activities as an agent of a foreign power and that his own conduct is assisting or furthering such activities. The innocent dupe who unwittingly aids a foreign intelligence officer cannot be targeted under this provision.¹⁴⁶

The third category, which considers a U.S. person to be “an agent of a foreign power” for knowingly entering the country under false or fraudulent identity, almost always involves a showing of criminality, simply because it is not possible to legally enter the United States without providing proof of one’s identity to a government official.¹⁴⁷ It is similarly illegal to knowingly assume a false identity under anti-fraud provisions of the U.S. Code.¹⁴⁸

FISA’s deliberate engagement of criminal law provisions and standards has been acknowledged by the government in defense of bringing down the wall between prosecution and investigation:

[A] U.S. person may not be an “agent of a foreign power” unless he engages in activity that either is, may be, or would be a crime if committed against the United States or within U.S. jurisdiction. Although FISA does not always require a showing of an imminent crime or “that the elements of a specific offense exist,” Senate Intelligence Report at 13, it does require the government to establish probable cause to believe that an identifiable target is knowingly engaged in terrorism, espionage, or clandestine intelligence activities or is knowingly entering the country with a false identity or assuming one once inside the country on behalf of a foreign power. Thus, while FISA imposes a more relaxed criminal

145. Compare *id.*, with 18 U.S.C. §§ 2, 371 (2006) (requiring actor to be engaged in the illegal action himself or working with another to commit the offense); see also Supplemental Brief for the United States, *supra* note 138.

146. H.R. REP. NO. 95-1283, pt. 1, at 44 (1978).

147. 18 U.S.C. § 1001.

148. *Id.* § 1028.

probable cause standard than Title III, those differences are not extensive as applied to U.S. persons.¹⁴⁹

The government cannot have it both ways: either U.S. persons have heightened protections under FISA—protections that rise to the level of those provided under Title III—or they do not.

Congress provided further protections for U.S. persons. The statute limited the breadth of surveillance operations by requiring that probable cause could not be established solely on the basis of otherwise protected First Amendment activity.¹⁵⁰ This was meant to ensure that the executive branch could not place U.S. citizens under surveillance simply for exercising their First Amendment rights.

3. *Minimization Procedures for Acquisition and Retention*

A third protection inserted by Congress centered on the introduction of minimization procedures to protect activity not related to foreign intelligence from government scrutiny.¹⁵¹ The legislature insisted here on minimizing not just the analysis of the information, but its “*acquisition and retention.*”¹⁵² Specifically, according to the statute:

“Minimization procedures”, with respect to electronic surveillance, means—

- (1) specific procedures, which shall be adopted by the Attorney General, that are reasonably designed in light of the purpose and technique of the particular surveillance, to minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons¹⁵³

Under FISA, only U.S. persons’ information must be subject to minimization procedures.¹⁵⁴

149. Supplemental Brief for the United States, *supra* note 138, at 28.

150. 50 U.S.C. § 1805(a)(2).

151. *Id.* § 1804(a)(4).

152. *Id.* § 1801(h) (emphasis added).

153. *Id.*

154. *Id.*

4. *Establishment of the Foreign Intelligence Surveillance Court and Court of Review*

As a further precaution against executive overreach, Congress provided in FISA for two courts: the Foreign Intelligence Surveillance Court and the Foreign Intelligence Surveillance Court of Review (FISCR).

As aforementioned, a key principle throughout the debates was the importance of heightened protections where U.S. persons' information may be involved. The conference was deadlocked on how best to accomplish this, until the Senate receded and accepted the House language exempting certain particularly sensitive surveillance (that is, relating solely to foreign powers) from judicial review. The decision rested on the grounds that (1) such surveillance did not involve U.S. persons; and (2) having removed the most sensitive information from external review, the Foreign Intelligence Surveillance Court could be given a greater role in protecting the rights of each U.S. person targeted by the government.¹⁵⁵ The use of a judicial element went some way towards providing for an independent, neutral, disinterested magistrate to review the strength of the government's case supporting the initiation of surveillance.¹⁵⁶

Initially, the statute provided for seven judges to sit on FISC. That number has since expanded to include eleven judges drawn from at least seven of the federal circuits, three of whom must reside in the Washington, D.C. area.¹⁵⁷ Both the FISC judges and the judges on FISCR are selected by the Chief Justice of the U.S. Supreme Court.¹⁵⁸ To avoid agency capture, judges only may serve for up to seven years, at the conclusion of which they are not eligible to serve again as FISC judges.¹⁵⁹

From the beginning, FISC's role was limited: it was merely to grant or to deny applications for orders.¹⁶⁰ The statute included detailed instructions about what must be included in such applications: the identity of the federal officer making the applica-

155. 124 CONG. REC. 36,409 (1978).

156. Discussion with former members of the Church Committee, in Washington, D.C. (Sept. 23, 2013).

157. 50 U.S.C. § 1803(a)(1).

158. *Id.* § 1803(a)(1)–(b).

159. *Id.* § 1803(d).

160. *Id.* § 1803(a).

tion; the identity, if known, of the target; a statement of the facts and circumstances relied upon to justify the applicant's belief that the target is a foreign power or an agent of a foreign power and that each of the facilities or places at which electronic surveillance is directed is being (or about to be) used by a foreign power or an agent thereof; a statement of the proposed minimization procedures; a description of the nature of the information sought; a certification from an executive branch official; a summary statement of the means by which the surveillance will be effected; a statement of the facts concerning all previous applications; and a statement of the period of time for which the surveillance is required to be maintained.¹⁶¹

Where the government has met the necessary criteria, the judge's role is to enter an *ex parte* order as requested or to modify it accordingly. Initially, such orders could be issued only in relation to electronic surveillance. Subsequent amendments expanded FISC's jurisdiction to physical searches, pen registers and trap and trace devices, searches of business records, and tangible things.¹⁶² These alterations, however, were in substance and not in form. The function being performed by FISC throughout was the same: to grant or to deny orders prior to the acquisition of information on particular targets.

C. Subsequent Amendment

Since FISA's introduction, Congress has amended the statute to cover physical searches,¹⁶³ pen register and trap and trace devices,¹⁶⁴ searches of business records,¹⁶⁵ and tangible goods.¹⁶⁶

161. *Id.* § 1804(a).

162. *Id.* §§ 1821–1824 (orders for physical search); *id.* § 1842 (pen register and trap and trace devices); *id.* § 1861 (business records and tangible goods).

163. Intelligence Authorization Act for Fiscal Year 1995, Pub. L. No. 103-359, § 302(c), 108 Stat. 3423, 3445 (1994) (codified at 50 U.S.C. §§ 1821–1829).

164. Intelligence Authorization Act for Fiscal Year 1999, Pub. L. No. 105-272, § 601, 112 Stat. 2396, 2404–2410 (1998) (codified at 50 U.S.C. §§ 1841–1846).

165. *Id.* § 602, 112 Stat. at 2410.

166. Various further amendments of these sections have been enacted. The USA PATRIOT Act, for instance, changed the duration of certain FISA authorization orders (§ 207), increased the number of FISC judges to 11 (§ 208); amended FISA pen register and trap and trace provisions (§ 214), changed the purpose of electronic & physical searches (§ 218), and authorized coordination between intelligence and law enforcement (§ 504). Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA

Because of their consistent structure and approach, these provisions have come to be referred to collectively as “traditional FISA.”¹⁶⁷ A brief discussion of the subsequent amendments helps to underscore Congress’s general approach and to elucidate ways in which the bulk collection of U.S. persons’ metadata violates the orientation of the statute and, as addressed in Part II, the statutory language.

1. *Physical Search, Pen-Trap*

Similar to the electronic surveillance provisions, physical search orders under FISA are limited by the requirement that the government establish the target of the search before acquiring the information. Specifically, physical search orders may be used only to target “premises, information, material, or property used exclusively by, or under the open and exclusive control of, a foreign power or powers.”¹⁶⁸ The subsection adopts the same definitions of “foreign power,” “agent of a foreign power,” “international terrorism,” “sabotage,” “foreign intelligence information,” and “United States person” as used elsewhere in the statute.¹⁶⁹ It provides for FISC to grant or to deny orders consistent with FISC’s role in electronic surveillance.¹⁷⁰ The

PATRIOT Act) Act of 2001, Pub. L. No. 107-56, 115 Stat. 272. ITRPA subsequently added a “lone wolf” provision via § 60001(a).

167. *See, e.g.*, 1 DAVID S. KRIS & J. DOUGLAS WILSON, NATIONAL SECURITY INVESTIGATIONS & PROSECUTIONS, ch. 12 (2d ed. 2012). In addition to the aforementioned amendments, in 2001 Congress amended FISA to take account of roving wiretaps. USA PATRIOT Act § 206, 115 Stat. at 282 (amending § 105(c)(2)(B) of the Foreign Intelligence Surveillance Act of 1978, codified as amended at 50 U.S.C. § 1805(c)(2)(B)). This alteration reflected a change that had been integrated into criminal law measures in 1998. At that time, the House Conference Report explained:

Under current law, judges issue wiretap orders authorizing law enforcement officials to place a wiretap on a specific telephone number. Criminals, including terrorists and spies, know this and often try to avoid wiretaps by using pay telephones on the street at random, or by using stolen or cloned cell telephones. As law enforcement officials cannot know the numbers of these telephones in advance, they are unable to obtain a wiretap order on these numbers from a judge in time to intercept the conversation, and the criminal is able to evade interception of his communication.

H.R. REP. NO. 105-780, at 32 (1998) (Conf. Rep.).

168. 50 U.S.C. § 1822(a)(1)(A)(i).

169. *Id.* § 1821(1).

170. *Id.* §§ 1822–1824.

government must make the same showings, particularly describing the target prior to FISC granting the order.¹⁷¹ Heightened protections are afforded to U.S. persons.¹⁷²

In 1998, Congress amended FISA to allow for the installation and use of pen register (recording numbers dialed from a particular phone) and trap and trace devices (acting as a caller ID record).¹⁷³ The Attorney General, or a designated attorney, must submit an application in writing and under oath either to FISC or to a magistrate specifically appointed by the Chief Justice to hear pen register or trap and trace applications on behalf of the FISA court.¹⁷⁴ Similar to the provisions related to electronic communications and physical search, the application must include information to show that the device has been, or will in the future be, used by someone who is engaging, or has engaged, in international terrorism or is a foreign power or agent thereof.¹⁷⁵ In the event of an emergency, the Attorney General can authorize the installation and use of a pen register or trap and trace device without judicial approval.¹⁷⁶ Nevertheless, a proper application must be made to the appropriate judicial authority within seven days.¹⁷⁷

Following the 9/11 attacks, Congress relaxed the requirement for factual proof for placement of a pen or trap. The applicant no longer must demonstrate why he or she believes that an individual engaged in international terrorism will use a telephone line. Instead, the applicant must demonstrate only that the information likely to be gained does not directly concern a

171. *Id.* § 1823.

172. *See, e.g., id.* § 1822(1)(A)(ii) (requiring the Attorney General to certify in writing and under oath that “there is no substantial likelihood that the physical search will involve the premises, information, material, or property of a United States Person”); *id.* § 1822(1)(A)(iii) (requiring minimization procedures for U.S. persons’ information).

173. Intelligence Authorization Act for Fiscal Year 1999, Pub. L. No. 105-272, §§ 601–602, 112 Stat. 2396, 2404 (1998); 50 U.S.C. §§ 1841–1846 (pen and trap); *id.* §§ 1861–1862 (tangible things).

174. 50 U.S.C. § 1842(a)–(b).

175. As with the application for electronic surveillance, the applicant must include the name of the official seeking surveillance, as well as certification that “the information likely to be obtained is relevant to an ongoing foreign intelligence or international terrorism investigation.” *Id.* § 1842(c)(1)–(2).

176. *Id.* § 1843(a).

177. *Id.* § 1843(a)(2).

U.S. person and will be relevant to protection against international terrorism.¹⁷⁸ This provision, hotly contested by civil libertarians, was scheduled to sunset on December 31, 2005,¹⁷⁹ but in 2006 Congress made it permanent.¹⁸⁰ Although the provision relaxes the standard for obtaining information from particular telephone lines, it still establishes a higher bar for obtaining U.S. persons' information.

The statute understands the terms "pen register" and "trap and trace device" consistent with the criminal law standard defining a pen register as:

[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.¹⁸¹

A "trap and trace device" is defined as:

[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.¹⁸²

In addition to all dialing, routing, addressing, and signaling information sent from or received by a target, orders may require electronic communication service providers to disclose further information, including:

- (I) the name of the customer or subscriber;
- (II) the address of the customer or subscriber;
- (III) the telephone or instrument number, or other subscriber number or identifier, of the customer or subscriber,

178. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT Act) Act of 2001, Pub. L. No. 107-56, 115 Stat. 272, 287.

179. USA PATRIOT Act § 215, 115 Stat. at 287 (codified as amended at 50 U.S.C. § 1861 (2000 & Supp. V 2001)); *id.* § 224, 115 Stat. at 295 (codified as amended at 18 U.S.C. § 2510 (2000 & Supp. V 2001) (note)).

180. USA PATRIOT Improvement and Reauthorization Act of 2005, Pub. L. No. 109-177, § 102, 120 Stat. 192 (2006).

181. 18 U.S.C. § 3127(3) (2006 & Supp. V 2011).

182. *Id.* § 3127(4).

- including any temporarily assigned network address or associated routing or transmission information;
- (IV) the length of the provision of service by such provider to the customer or subscriber and the types of services utilized by the customer or subscriber;
 - (V) in the case of a provider of local or long distance telephone service, any local or long distance telephone records of the customer or subscriber;
 - (VI) if applicable, any records reflecting period of usage (or sessions) by the customer or subscriber; and
 - (VII) any mechanisms and sources of payment for such service, including the number of any credit card or bank account utilized for payment for such service.¹⁸³

These provisions are consistent with Congress's approach in FISA: namely, particularized showing in relation to the target, a decision prior to the collection of information, issuance of an individualized order by the court, and heightened protections for U.S. persons.

2. *Business Records, Tangible Goods, and Section 215*

Following the Oklahoma City bombing, in 1998 Congress amended FISA to authorize the production of certain kinds of business records of those suspected of being foreign powers or agents of a foreign power: namely, documents maintained by common carriers, public accommodation facilities, storage facilities, and vehicle rental facilities.¹⁸⁴ Any records obtained under this provision had to be for "an investigation to gather foreign intelligence information or an investigation concerning international terrorism."¹⁸⁵ The application had to include "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."¹⁸⁶

As with the other provisions of traditional FISA, Congress assigned the terms "foreign power," "agent of a foreign power,"

183. 50 U.S.C. § 1842(d)(2)(C)(i).

184. Intelligence Authorization Act for Fiscal Year 1999, Pub. L. 105-272, § 602, 112 Stat. 2396, 2410 (1998).

185. *Id.*

186. *Id.*

“foreign intelligence information,” and “international terrorism” the same meanings as employed in relation to electronic surveillance.¹⁸⁷ Congress also required intelligence agencies to follow the same steps as those taken with regard to electronic surveillance (i.e., to submit an application to FISC to obtain an order, which then compels the companies to hand over the records).¹⁸⁸

Initially, the FBI did not heavily rely on the business records provision. Between 1998 and 2001, the FBI used it only once. Nevertheless, in 2001 Congress expanded the types of records that could be obtained, authorizing intelligence agencies to apply for an order from FISC “requiring the production of any tangible things (including books, records, papers, documents, and other items).”¹⁸⁹ Congress eliminated restrictions on the types of businesses or entities on which such an order could be served.¹⁹⁰ It retained, however, the general contours of FISA, specifying that such items be obtained in the course of “an investigation to protect against international terrorism or clandestine intelligence activities.”¹⁹¹ Congress again added heightened protections for U.S. persons, requiring that such investigations, where directed towards a U.S. person, “not be

187. *Id.*

188. *Id.*

189. USA PATRIOT Act, Pub. L. No. 107-56, § 215, 115 Stat. 272, 287. Congress also amended FISA to require that applicants to FISC certify that “a significant purpose of the surveillance is to obtain foreign intelligence.” 50 U.S.C. § 1804(a)(6)(B) (2006 & Supp. V 2011). This shift, from the prior language that “the” purpose be to obtain foreign intelligence, had the effect of removing a wall that had built up within the Department of Justice between intelligence officers and criminal prosecutors. The government argued that the latter should be allowed to advise the former concerning the initiation, operation, continuation, or expansion of FISA searches or surveillance. *In re All Matters Submitted to the Foreign Intelligence Surveillance Court*, 218 F. Supp. 2d 611, 623 (FISA Ct. 2002). The Foreign Intelligence Surveillance Court of Review upheld the change. *See In re Sealed Case*, 310 F.3d 717 (FISA Ct. Rev. 2002). This alteration, however, simply recognizes parallels between criminal violations and national security threats. It does not suddenly shift the focus of the statute to allow intelligence agencies to collect information on millions of Americans not suspected of any wrongdoing.

190. Compare USA PATRIOT Act § 215, 115 Stat. at 287, with Intelligence Authorization Act for Fiscal Year 1999, Pub. L. No. 105-272, § 602, 112 Stat. 2396, 2410 (1998).

191. *Id.*

conducted . . . solely upon the basis of activities protected by the first amendment to the Constitution.”¹⁹²

In the new statute, Congress eliminated the requirement that the application include “specific and articulable facts” indicating that the individual to whom the records pertain is a foreign power or an agent thereof.¹⁹³ Nevertheless, from the beginning the Department of Justice rightly understood that the scope of information obtainable under the tangible goods provision was still narrow, in that the information must pertain directly to the person targeted in the authorized investigation. A memorandum sent in October 2003 to all Field Offices explained:

The business records request is not limited to the records of the target of a full investigation. The request must simply be sought for a full investigation. Thus, if the business records relating to one person are relevant to the full investigation of another person, those records can be obtained by a FISC order despite the fact that there is no open investigation of the person to whom the subject of the business records pertain.¹⁹⁴

The relevance standard adopted was thus specific with regard to the connection between the records sought and the target of the investigation, as well as limited with regard to the actual establishment of a particular investigation.

For the first two years, Attorney General guidelines allowed business record requests only as part of full field investigations. But in 2003, in the same memo specifying that the records must be directly related to the person under investigation, the General Counsel of the National Security Law Unit indicated that the type of investigation that must already be established, and to which the records being sought must pertain, “may be revised in the near future to allow the use of a FISC business records order in a preliminary investigation.”¹⁹⁵ “Near future” indeed: two days later, on October 31, 2003, the Attorney General issued a

192. Compare USA PATRIOT Act § 215, 115 Stat. at 287, with Intelligence Authorization Act for Fiscal Year 1999 § 602, 112 Stat. at 2410.

193. USA PATRIOT Act § 215, 115 Stat. at 287.

194. FBI Memorandum from General Counsel, National Security Law Unit, to All Field Offices, Business Records Orders Under 50 U.S.C. § 1861 (Oct. 29, 2003), available at http://epic.org/privacy/terrorism/usapatriot/foia/field_memo.pdf, [<http://perma.cc/0LD8wREXHF1>].

195. *Id.*

thirty-eight page document establishing new guidelines for national security investigations—and allowing agents to obtain business records during preliminary investigations.¹⁹⁶

Despite the expansion to preliminary investigations, the specificity embedded in the relevance principle remained. To open a preliminary investigation, the Attorney General required in his 2003 guidelines that, *inter alia*, the individual targeted in the investigation be an international terrorist or an agent of a foreign power, or any individual, group, or organization engaged in activities constituting a threat to national security for, or on behalf of, a foreign power, or may be the target of a recruitment or infiltration effort by an international terrorist, foreign power, or an agent of a foreign power.¹⁹⁷

There are two points to make about this novel construction. First, the Attorney General emphasized particular “individuals,” “groups,” or “organizations” as the targets of preliminary investigations. This was consistent with FISA’s traditional approach. Second, only once a preliminary investigation was established could agents then make use of “authorized techniques” to obtain information (e.g., mail opening, physical search, or electronic surveillance requiring judicial order or warrant).¹⁹⁸ This meant that the target had to be determined (in the course of which the FBI would open a preliminary investigation) *before* orders allowing for the acquisition of tangible goods could issue.

Section 215 of the USA PATRIOT Act, the tangible goods provision, was set to expire December 31, 2005.¹⁹⁹ Congress has since renewed it seven times.²⁰⁰ It is now set to expire June 1,

196. See The Attorney General’s Guidelines for FBI National Security Investigations and Foreign Intelligence Collection 3–4, 15 (Oct. 31, 2003), available at <http://www.fas.org/irp/agency/doj/fbi/nsiguidelines.pdf>, [<http://perma.cc/0rvAkw2hfHR>].

197. *Id.* at 14.

198. *Id.* at 15.

199. USA PATRIOT Act, Pub. L. No. 107-56, § 224, 115 Stat. 272, 295 (2001).

200. See An Act to Amend the USA PATRIOT Act to Extend the Sunset of Certain Provisions of that Act and the Lone Wolf Provision of the Intelligence Reform and Terrorism Prevention Act of 2004 to July 1, 2006, Pub. L. No. 109-160, 119 Stat. 2957 (2005) (extension until Feb. 3, 2006); An Act To Amend the USA PATRIOT Act to Extend the Sunset of Certain Provisions of Such Act, Pub. L. No. 109-170, 120 Stat. 3 (2006) (extension until Mar. 10, 2006); USA PATRIOT Improvement and Reauthorization Act of 2005, Pub. L. No. 109-177, 120 Stat. 192 (2006) (extension until Dec. 31, 2009);

2015.²⁰¹ In 2005, in the course of extending Section 215, Congress added language tying the section more closely to FISA's overarching structure. It required applicants to submit a statement of facts establishing "reasonable grounds to believe that the tangible things sought are relevant to an authorized investigation (other than a threat assessment)."²⁰² The investigation to which the order is tied must be conducted under guidelines approved by the Attorney General.²⁰³ The purpose of the investigation must be "to obtain foreign intelligence information not concerning a United States person or to protect against international ter-

Department of Defense Appropriations Act, 2010, Pub. L. No. 111-118, 123 Stat. 3409 (2009) (allowing for a short-term, sixty day extension of 50 U.S.C. § 1861 until February 28, 2010); An Act to Extend Expiring Provisions of the USA PATRIOT Improvement and Reauthorization Act of 2005 and Intelligence Reform and Terrorism Prevention Act of 2004 until February 28, 2011, Pub. L. No. 111-141, 124 Stat. 37 (2010) (extension until Feb. 28, 2011); FISA Sunsets Extension Act of 2011, Pub. L. No. 112-3, 125 Stat. 5 (extension until May 27, 2011); PATRIOT Sunsets Extension Act of 2011, Pub. L. No. 112-14, 125 Stat. 216 (extension until June 1, 2015).

201. PATRIOT Sunsets Extension Act of 2011, Pub. L. No. 112-14, 125 Stat. 216. Note that in a race against the clock, President Obama signed the most recent, four-year extension of Section 215 just minutes before the midnight deadline, May 26, 2011. *Patriot Act extension signed into law despite bipartisan resistance in Congress*, WASH. POST, May 27, 2011, http://www.washingtonpost.com/politics/patriot-act-extension-signed-into-law-despite-bipartisan-resistance-in-congress/2011/05/27/AGbVlsCH_story.html, [http://perma.cc/0q4UyoJK3EU]. A bipartisan group of lawmakers had rallied against the measure, with the result that the USA PATRIOT Sunsets Extension Act of 2011 passed the Senate 72 to 23 and the House 250 to 153. With President Obama at a summit in France, the White House took the unusual step of having him sign the bill with an autopen—prompting commentators to question whether it was legal under Art. I, § 7 of the U.S. Constitution. See, e.g., *Originalism and the Autopen: Obama's "Signing" of Patriot Act Extension Constitutional*, CONSTITUTIONAL LAW PROF BLOG (May 30, 2011), <http://lawprofessors.typepad.com/conlaw/2011/05/originalism-and-the-autopen.html>, [http://perma.cc/09EN7mYcRaW]. The White House apparently relied on a memorandum opinion issued by the Office of Legal Counsel in 2005. See Memorandum Opinion from the Office of Legal Counsel to the President, *Whether the President May Sign a Bill by Directing that his Signature be Affixed to It* (July 7, 2005), available at http://lawprofessors.typepad.com/files/opinion_07072005.pdf, [http://perma.cc/0YSughFJSVz].

202. USA PATRIOT Improvement and Reauthorization Act of 2005 § 106, 120 Stat. at 196 (codified as amended at 50 U.S.C. § 1861 (2006)).

203. 50 U.S.C. § 1861(a)(2)(A). Such guidelines are issued consistent with Executive Order 12,333. In 2008, the Department of Justice issued new, consolidated guidelines. Attorney General's Guidelines for Domestic FBI Operations (Oct. 3, 2008), available at <http://www.justice.gov/ag/readingroom/guidelines.pdf>, [http://perma.cc/0GfT5Uq7Wro].

rorism or clandestine intelligence activities.”²⁰⁴ The underlying investigation may not be directed at a U.S. person based solely on otherwise protected First Amendment activity.²⁰⁵

Tangible things are presumptively relevant to an investigation where they pertain to: (1) “a foreign power or an agent of a foreign power”; (2) “the activities of a suspected agent of a foreign power,” themselves the subject of an authorized investigation; or (3) “an individual in contact with, or known to, a suspected agent of a foreign power who is the subject of an authorized investigation.”²⁰⁶

For certain materials—namely, “library circulation records, library patron lists, book sales records, book customer lists, firearms sales records, tax return records, educational records, or medical records”—with information identifying an individual, only the Director of the FBI, the Deputy Director of the FBI, or the Executive Assistant Director for National Security may make the application; none of these individuals may further delegate their authorities in this respect.²⁰⁷

In the 2005 amendments, Congress required “an enumeration of the minimization procedures” related to the retention and dissemination of any tangible things obtained.²⁰⁸ Any orders issued “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.”²⁰⁹ As discussed below, the telephony metadata program, by FISC’s own admission, fails to satisfy this statutory requirement.²¹⁰

204. USA PATRIOT Improvement and Reauthorization Act of 2005 § 106, 120 Stat. at 196 (codified as amended at 50 U.S.C. § 1861).

205. 50 U.S.C. § 1861(a)(2)(B).

206. *See id.* § 1861(b)(2)(A); *id.* § 1861(c)(1).

207. *Id.* § 1861(a)(3).

208. *Id.*

209. *Id.* § 1861(c)(2)(D).

210. Any individual served with an order is gagged from telling anyone other than individuals to whom disclosure is necessary to comply with the order or an attorney to obtain legal advice or help with regard to producing the items sought. *Id.* § 1861(d). Under the statute, an individual on whom an order has been served may challenge the legality of the order by filing a petition with the court within a year, requesting that the order be modified or set aside. *Id.* § 1861(f)(2)(A)(i).

D. *Broad Surveillance in Place of Particularization*

The telephony metadata program lacks the particularization that marks Congress's approach to domestic foreign intelligence gathering in FISA. The statute rejects the wholesale collection of domestic information. It relies on the *prior* targeting of foreign intelligence targets to justify surveillance. It provides U.S. persons a heightened level of protection. And it seeks to minimize the acquisition (not just the retention and dissemination) of information.

1. *Wholesale Collection of Information*

Project MINARET, which represented precisely the type of surveillance program that FISA was designed to forestall, was not nearly as extensive as the telephony metadata program. Over the course of Project MINARET, for instance, the watch list included approximately 1650 U.S. citizens in total.²¹¹ At no time were there more than 800 U.S. citizens' names on the list, out of a population of about 200 million Americans.²¹²

Today, in contrast, there are approximately 316 million Americans, a significant number of which have access to mobile devices.²¹³ Verizon, which is only one of the telecommunications companies served with a FISC order, is estimated to have a market share of 31.3% of the total number of wireless subscribers.²¹⁴ As of October 2013, this translated into 101.2 million wireless accounts.²¹⁵ This number eclipses the total number of U.S. citizens subject to the most egregious programs previously operated by the NSA, which gave rise to FISA in the first place.

The telephony program also goes substantially beyond the previous surveillance operation in its focus on calls of a purely

211. 5 *Church Committee Report*, *supra* note 38, at 33 (testimony of Lieutenant General Lew Allen, Jr., Director, National Security Agency).

212. *Id.* at 30, 33–34.

213. *U.S. and World Population Clock*, UNITED STATES CENSUS BUREAU, <http://www.census.gov/popclock/>, [<http://perma.cc/NN4C-R3LM>] (last visited Mar. 20, 2014).

214. Kyle Woodley, *Don't Sweat a BUD Monopoly*, INVESTORPLACE (Jan. 14, 2013), http://investorplace.com/2013/01/dont-sweat-a-bud-monopoly/#.Uu_OVI5xKPC, [<http://perma.cc/4EPZ-6PC3>].

215. Roger Cheng, *Verizon posts \$2.23B profit, adds 1.1M wireless connections*, CNET (Oct. 17, 2013), [http://news.cnet.com/8301-1035_3-57607860-94/verizon-posts-\\$2.23b-profit-adds-1.1m-wireless-connections/](http://news.cnet.com/8301-1035_3-57607860-94/verizon-posts-$2.23b-profit-adds-1.1m-wireless-connections/), [<http://perma.cc/J4XN-QXGD>].

local nature. According to the Director of the National Security Agency, Project MINARET did not monitor entirely domestic conversations.²¹⁶ The FISC Order issued in April 2013, however, specifically *requires* the collection of information “wholly within the United States, including local telephone calls.”²¹⁷ Set to expire on July 19, 2013, the Office of the Director of National Intelligence has confirmed that FISC has again renewed the order.²¹⁸

As discussed above, Congress designed the statute to be used in *specific cases* of foreign intelligence gathering. By limiting the targets of electronic surveillance, requiring probable cause, disallowing investigations solely on the basis of otherwise protected First Amendment activities, and insisting on minimization procedures, Congress sought to restrict agencies’ ability to violate U.S. citizens’ privacy. The business records provision built on this approach, adopting the *same definitions* that prevailed in other portions of the statute and requiring that agencies obtain orders to collect information on individuals believed to be foreign powers or agents of a foreign power. Congress later deliberately inserted “relevant” into the statute to ensure the continued specificity of targeted investigations.

In addition, Congress empowered FISC to consider each instance of placing an electronic wiretap. The NSA’s program, in contrast, delegates such oversight to the Executive, leaving all further inquiries of the databases to the agency involved. Once the NSA collects the telephony metadata, it is the NSA (and not FISC) that decides which queries to use, and which individuals to target within the database.

This change means that FISC is not performing its most basic function: protecting U.S. persons from incursions into their privacy. Instead, it leaves the determination of whom to target to the agency’s discretion. Traditional FISA depends upon the criteria in the statute being met *before* collection of information.

216. See 5 *Church Committee Report*, *supra* note 38, at 36.

217. *In re* Application of the Fed. Bureau of Investigation for an Order Requiring the Prod. of Tangible Things from Verizon Bus. Network Servs., Inc., Secondary Order, No. BR 13-80, at 2 (FISA Ct. Apr. 25, 2013).

218. See Press Release, Office of the Dir. of Nat’l Intelligence, Foreign Intelligence Surveillance Court Renews Authority to Collect Telephony Metadata (July 19, 2013), available at <http://www.dni.gov/index.php/newsroom/press-releases/191-press-releases-2013/898-foreign-intelligence-surveillance-court-renews-authority-to-collect-telephony-metadata>, [<http://perma.cc/0tZiDuzYCvX>].

That is, the authorities apply at the moment data is acquired—not when it is subsequently analyzed for more information. Although the government argues that intelligence is not acquired until it is mined for more information, or until a human operator is involved in the analysis, this view is neither expressed in the relevant statutory language nor congruent with the government’s own internal position.²¹⁹

2. *Absence of Prior Targeting*

The government has indicated that the information obtained from this program is important because, “by analyzing it, the Government can determine whether known or suspected terrorist operatives have been in contact with other persons who may be engaged in terrorist activities, including persons and activities within the United States.”²²⁰ The government sees the enormous number of records as central to the success of the program.²²¹ Once the records are obtained—once the “haystack” is created—the government can then go about finding out who the threats are—the proverbial needles in the haystack.²²²

This process is backwards. The whole point of FISA is for the government to first identify the target, and then to use this identification to obtain information. In contrast, the government is now arguing that it can obtain information as a way of figuring out who the targets should be. This directly contradicts FISA’s design.

219. See, e.g., Eric H. Holder, Jr., Att’y General of the United States, *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 1* (Jan. 8, 2007), available at <http://epic.org/2013/06/nsa-targeting-and-minimization.html>, [<http://perma.cc/0PKxzba3aiL>] (“Acquisition means the collection by NSA or the FBI through electronic means of a non-public communication to which it is not an intended party.”).

220. SECTION 215 WHITE PAPER, *supra* note 2, at 1.

221. *Id.* at 4 (“It would be impossible to conduct these queries effectively without a large pool of telephony metadata to search, as there is no way to know in advance which numbers will be responsive to the authorized queries.”).

222. See, e.g., *How Disclosed NSA Programs Protect Americans, and Why Disclosure Aids Our Adversaries: Hearing Before the H. Permanent Select Comm. on Intelligence*, 113th Cong. (2013) (statement of James Cole, Deputy Att’y Gen.), available at <http://intelligence.house.gov/video/how-disclosed-nsa-programs-protect-americans-and-why-disclosure-aids-our-adversaries>, [<http://perma.cc/0NeE3FAYFbT>].

3. *No Higher Threshold for U.S. Persons*

In addition, as detailed above, there are myriad ways in which FISA creates extra protections for U.S. persons. In light of the historical context, the reason for this is clear. The statute arose from revelations about the cavalier manner in which the intelligence agencies were treating Americans' right to privacy. New protections thus centered on creating higher standards for *targeting* U.S. persons, as well as for later analysis and dissemination of U.S. persons' information.

Outside of minimization procedures relating to the downstream manipulation and dissemination of information, however, the telephony metadata program does not recognize a higher protection for U.S. persons at the moment of data acquisition. The failure to create higher standards thus runs counter to the approach Congress adopted in passing FISA.

E. Role of the Foreign Intelligence Surveillance Court

In at least three important ways, FISC no longer serves the purpose for which it was designed. First, Congress created the court to determine whether the executive branch had met its burden of demonstrating that there was sufficient evidence to target individuals within the United States, prior to collection of such information. The telephony metadata program demonstrates that FISC has abdicated this responsibility to the executive branch generally, and to the NSA in particular. Continued noncompliance underscores concern about relying on the intelligence community to protect the Fourth Amendment rights of U.S. persons.

Second, Congress did not envision a lawmaking role for FISC. Its decisions were not to serve as precedent, and FISC was not to offer lengthy legal analyses, crafting in the process, for instance, exceptions to the Fourth Amendment warrant requirement or defenses of wholesale surveillance programs.

Third, questions have recently been raised about the extent to which FISC can fulfill the role of being a neutral, disinterested magistrate. Congress went to great lengths, for instance, to try to ensure diversity on the court. To the extent that the appointments process implies an ideological predilection, at a minimum, it is worth noting that almost all of the judges who serve on FISC and FISCR are Republican appointees. The rate of applications being granted, in conjunction with the in cam-

era and ex parte nature of the proceedings, also raises questions about the extent to which FISC serves as an effective check on the executive branch. The lack of technical expertise of those on the court further introduces questions about the judges' ability to understand how the authorities they are extending to the NSA are being used.

1. *Reliance on NSA to Ascertain Reasonable, Articulable Suspicion*

In 1978 Congress created FISC to serve as a neutral, disinterested observer. In this capacity, one of its principal responsibilities was to ascertain whether the government had demonstrated probable cause that individuals to be targeted under FISA were foreign powers or agents thereof, and likely to use the facilities to be placed under surveillance. As was previously discussed, consistent with this approach, in 1998 Congress introduced the business records provision, requiring in the process that the government submit a statement of "specific and articulable facts" to the court in support of its application. Although the showing was eliminated in 2001, four years later Congress re-introduced a requirement that the government submit a statement of facts establishing "reasonable grounds to believe that the tangible things" to be obtained are "relevant to an authorized investigation." This language puts the court in the position of verifying whether the government has met its burden of proof prior to intelligence collection. The court, however, no longer serves in this function.

To the contrary, FISC's primary order authorizing the collection of telephony metadata required that designated *NSA officials* make a finding that there is "reasonable, articulable suspicion" (RAS) that a seed identifier proposed for query is associated with a particular foreign terrorist organization prior to its use. It is thus left to the executive branch to determine whether the executive branch has sufficient evidence to place individuals or entities under surveillance.

The dangers associated with the court removing itself from the process are clear. Documents recently released under court orders in a related FOIA case establish that for nearly three

years, the NSA did not follow these procedures²²³—even though numerous NSA officials were aware of the violation.²²⁴ Noncompliance incidents have continued. Collectively, these incidents raise serious question as to whether FISC is performing the functions for which it was designed.

a. Failure to Report Initial Noncompliance

Although the NSA had been contravening the order since May 2006, it was not until early 2009, when representatives of the Department of Justice met with NSA representatives to be briefed on the NSA's handling of the telephony metadata, that the illegal behavior was brought to FISC's attention.²²⁵ President Barack Obama took office on January 20, 2009; it appears that recognition of the noncompliance occurred during the transition. During the briefing and in subsequent discussions, DOJ representatives inquired about the alert process. Learning of the process being used, DOJ personnel expressed concern that the program had been misrepresented to FISC.²²⁶ The NSA had been using identifiers employed to collect information under Executive Order 12,333—not FISA—to search the telephony

223. See *In re Prod. of Tangible Things From [REDACTED]*, Order Regarding Preliminary Notice of Compliance Incident Dated Jan. 15, 2009, No. BR 08-13 (FISA Ct. Jan. 28, 2009), available at http://www.dni.gov/files/documents/section/pub_Jan%2028%202009%20Order%20Regarding%20Prelim%20Notice%20of%20Compliance.pdf, [<http://perma.cc/0soKuBTCNQL>]; see also *DNI Clapper Declassifies Intelligence Community Documents Regarding Collection Under Section 501 of the Foreign Intelligence Surveillance Act*, IC ON RECORD, (Sept. 10, 2013), <http://icontherecord.tumblr.com/post/60867560465/dni-clapper-declassifies-intelligence-community>, [<http://perma.cc/KDV2-3ZT6>].

224. Declaration of Lieutenant General Keith B. Alexander at 25–26, *In re Prod. of Tangible Things from [REDACTED]*, No. BR 08-13 (FISA Ct. Feb. 13, 2009), available at http://www.dni.gov/files/documents/section/pub_Feb%2012%202009%20Memorandum%20of%20US.pdf, [<http://perma.cc/0TjRzWGeXcT>] (listing seven people in the Signals Intelligence Directive, two from the Office of the General Counsel, and one additional person whose name has not been disclosed who knew, or may have known of the problem since May 2006). Three additional people from the General Counsel's office and from SID became aware of the use of non-RAS-approved identifiers via e-mail on May 25, 2006. *Id.* at 26. The DNI noted an additional "indeterminate number of other NSA personnel who knew or may have known the alert list contained both RAS and non-RAS selectors." *Id.* at 26.

225. *Id.* at 27–28.

226. *Id.* at 27.

database.²²⁷ This meant that the standards applying to foreigners were used in relation to U.S. persons.

227. NSA's general SIGINT authorities derive from (1) Exec. Order No. 12,333, § 1.7, 46 Fed. Reg. 59,941 (Dec. 4, 1981) (authorizing the NSA to "[c]ollect (including through clandestine means), process, analyze, produce, and disseminate signals intelligence information for foreign intelligence and counterintelligence purposes to support national and departmental missions"); (2) National Security Council Intelligence Directive 6, Foreign Wireless and Radio Monitoring (Dec. 12, 1947), available at http://www.foia.cia.gov/sites/default/files/document_conversions/50/NSCID_No_6_Foreign_Wireless_and_Radio_Monitoring_12_Dec_1947.pdf, [http://perma.cc/0dy3BfySG6k] (noting that the "DCI shall conduct all Federal monitoring of foreign propaganda and press broadcasts required for the collection of intelligence information to meet the needs of all Departments and Agencies in connection with the National Security" and that the DCI "shall disseminate such intelligence information to the various Departments and Agencies which have an authorized interest therein"); and (3) Department of Defense Directive 5100.20 (Jan. 26, 2010), available at <http://www.dtic.mil/whs/directives/corres/pdf/510020p.pdf>, [http://perma.cc/0uksdWff7fo] ("[T]he National Security Agency (NSA) is the U.S. Government (USG) lead for cryptology, and its mission encompasses both Signals Intelligence (SIGINT) and Information Assurance (IA) activities. The Central Security Service (CSS) conducts SIGINT collection, processing, analysis, production, and dissemination, and other cryptologic operations as assigned by the Director, NSA/Chief, CSS (DIRNSA/CHCSS). NSA/CSS provides SIGINT and IA guidance and assistance to the DoD Components, as well as national customers . . ."). In addition, some, but not all, of the SIGINT activities undertaken by NSA are governed by FISA. Declaration of Lieutenant General Keith B. Alexander at 34, *In re* Prod. of Tangible Things from [REDACTED], No. BR 08-13 (FISA Ct. Feb. 13, 2009), available at http://www.dni.gov/files/documents/section/pub_Feb%2012%202009%20Memorandum%20of%20US.pdf, [http://perma.cc/0TjRzWGeXcT].

When executing its SIGINT mission, NSA is only authorized to collect, retain, or disseminate information concerning U.S. persons consistent with Attorney General guidelines. The current procedures approved by the Attorney General are located in the DEPARTMENT OF DEFENSE, REGULATION 5240.1-R, PROCEDURES GOVERNING THE ACTIVITIES OF DOD INTELLIGENCE COMPONENTS THAT AFFECT UNITED STATES PERSONS 24–37, as well as a classified annex to the regulation overseeing the NSA's electronic surveillance. Declaration of Lieutenant General Keith B. Alexander at 34, *In re* Prod. of Tangible Things from [REDACTED], No. BR 08-13 (FISA Ct. Feb. 13, 2009), available at http://www.dni.gov/files/documents/section/pub_Feb%2012%202009%20Memorandum%20of%20US.pdf, [http://perma.cc/0TjRzWGeXcT].

To administer the program, the NSA constructed two lists: the first, an "alert list," includes all identifiers (foreign and domestic) of interest to counterterrorism analysts. Memorandum of the United States in Response to the Court's Order Dated Jan. 28, 2009 at 10, *In re* Prod. of Tangible Things from [REDACTED], No. BR 08-13 (FISA Ct. Feb. 17, 2009), available at http://www.dni.gov/files/documents/section/pub_Feb%2012%202009%20Memorandum%20of%20US.pdf, [http://perma.cc/0TjRzWGeXcT]. The second, the "station table," is a historical listing of all telephone identifiers that had undergone a reasonable, articulable suspicion determination, including the results. *Id.* But see Declaration of Lieutenant General Keith B. Alexander at 9, *In re* Prod. of Tangible Things from [RE-

The DOJ informed FISC within a week of the meeting that the government had been querying the business records in a manner that contravened both the original order and sworn statements of several executive branch officials.²²⁸ FISC was not amused. Judge Reggie Walton expressed concern “about what appears to be a flagrant violation of its Order in this matter.”²²⁹ The NSA had repeatedly misled FISC in its handling of the database.²³⁰ FISC immediately issued an order, directing the NSA to comprehensively review the agency’s handling of telephony metadata.²³¹ It gave the government until February 17, 2009 to file a brief to defend its actions and to help FISC to determine whether further action should be taken against the government or its representatives.²³²

The NSA initially admitted only “that NSA’s descriptions to [FISC] of the alert list process . . . were inaccurate and that the Business Records Order did not provide the Government with authority to employ the alert list in the manner in which it did.”²³³ It further acknowledged, “the majority of telephone

DACTED], No. BR 08-13 (FISA Ct. Feb. 13, 2009), *available at* http://www.dni.gov/files/documents/section/pub_Feb%2012%202009%20Memorandum%20of%20US.pdf, [<http://perma.cc/0TjRzWGeXcT>] (referring to the first source as the “Address Database” and describing it as “a master target database of foreign and domestic telephone identifiers”).

228. *In re* Prod. of Tangible Things From [REDACTED], Order Regarding Preliminary Notice of Compliance Incident Dated Jan. 15, 2009, No. BR 08-13, at 2 (FISA Ct. Jan. 28, 2009), *available at* http://www.dni.gov/files/documents/section/pub_Jan%2028%202009%20Order%20Regarding%20Prelim%20Notice%20of%20Compliance.pdf, [<http://perma.cc/0zB1dSnc7k5>].

229. *Id.* at 4.

230. *See, e.g.*, OFFICE OF THE INSPECTOR GEN., *supra* note 1 (see page 94 of 1846 and 1862 Production, Mar. 5, 2009) (“The management controls designed by the Agency to govern the processing, dissemination, data security, and oversight of telephony metadata and U.S. person information obtained under the Order are adequate and in several aspects exceed the terms of the Order.”).

231. *In re* Prod. of Tangible Things From [Redacted], Order Regarding Preliminary Notice of Compliance Incident Dated Jan. 15, 2009, No. BR 08-13 (FISA Ct. Jan. 28, 2009), *available at* http://www.dni.gov/files/documents/section/pub_Jan%2028%202009%20Order%20Regarding%20Prelim%20Notice%20of%20Compliance.pdf, [<http://perma.cc/0zB1dSnc7k5>].

232. *See id.* at 2.

233. Memorandum of the United States in Response to the Court’s Order Dated Jan. 28, 2009 at 1–2, *In re* Prod. of Tangible Things From [REDACTED], No. BR 08-13 (FISA Ct. Feb. 17, 2009), *available at* http://www.dni.gov/files/documents/section/pub_Feb%2012%202009%20Memorandum%20of%20US.pdf, [<http://perma.cc/0TjRzWGeXcT>].

identifiers compared against the incoming BR metadata in the rebuilt alert list were not RAS-approved.”²³⁴ The actual numbers, reported to FISC in February 2009, were staggering: as of January 15, 2009, “only 1,935 of the 17,835 identifiers on the alert list were RAS-approved.”²³⁵

It was not that the NSA was unaware of the requirements established by the statute and by FISC. The Attorney General had, consistent with the primary order, established minimization procedures, among which was the following:

Any search or analysis of the data archive shall occur only after a particular known telephone number has been associated with [REDACTED] More specifically, access to the archived data shall occur 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] organization; provided, however, that a telephone number believed to be used by a U.S. person shall not be regarded as associated with [REDACTED] solely on the basis of activities that are protected by the First Amendment to the Constitution.²³⁶

Nevertheless, apparently, neither the Signals Intelligence Directorate nor the Office of the General Counsel had caught the fact

234. *Id.* at 11; *see also id.* at 6. Note that the NSA refers to FISC-authorized Business Record metadata as “BR metadata.” *In re* Prod. of Tangible Things from [REDACTED], Order, No. BR 08-13, at 4 (FISA Ct. Mar. 2, 2009), *available at* http://www.dni.gov/files/documents/section/pub_March%202009%20Order%20from%20FISC.pdf, [<http://perma.cc/5KGD-SWMW>].

235. Memorandum of the United States in Response to the Court’s Order Dated Jan. 28, 2009 at 11, *In re* Prod. of Tangible Things From [REDACTED], No. BR 08-13 (FISA Ct. Feb. 17, 2009), *available at* http://www.dni.gov/files/documents/section/pub_Feb%2012%202009%20Memorandum%20of%20US.pdf, [<http://perma.cc/0TjRzWGeXcT>]; *see also* Declaration of Lieutenant General Keith B. Alexander at 8, *In re* Prod. of Tangible Things from [REDACTED], No. BR 08-13 (FISA Ct. Feb. 13, 2009), *available at* http://www.dni.gov/files/documents/section/pub_Feb%2012%202009%20Memorandum%20of%20US.pdf, [<http://perma.cc/0TjRzWGeXcT>].

236. Memorandum of the United States in Response to the Court’s Order Dated Jan. 28, 2009 at 4, *In re* Prod. of Tangible Things from [REDACTED], No. BR 08-13 (FISA Ct. Feb. 17, 2009), *available at* http://www.dni.gov/files/documents/section/pub_Feb%2012%202009%20Memorandum%20of%20US.pdf, [<http://perma.cc/0TjRzWGeXcT>], (citing Order, No. BR 06-05, at 5) (internal footnote omitted).

that nearly ninety percent of the queries to the bulk dataset had been illegal.²³⁷ Nor had they realized that their reports to FISC claiming that only RAS-approved numbers were being run against the bulk metadata were false.²³⁸

Meanwhile, the NSA had disseminated 275 reports to the FBI as a result of contact chaining and queries of NSA's archive of telephony metadata.²³⁹ Thirty-one of these had resulted directly

237. *Id.* at 11 ("Based upon NSA's recent review, neither NSA SID nor NSA OGC identified the inclusion of non-RAS-approved identifiers on the alert list as an issue requiring extensive analysis.").

238. *See, e.g.*, Memorandum of the United States in Response to the Court's Order Dated Jan. 28, 2009 at 13, *In re* Prod. of Tangible Things from [REDACTED], No. BR 08-13 (FISA Ct. Feb. 17, 2009) (quoting NSA Report to FISC at 12-15, *In re* Production of Tangible Things from [REDACTED], No. BR 06-05), available at http://www.dni.gov/files/documents/section/pub_Feb%2012%202009%20Memorandum%20of%20US.pdf, [<http://perma.cc/0TjRzWGeXcT>] ("As of the last day of the reporting period addressed herein, NSA had included a total of 3980 telephone numbers on the alert list, which include foreign numbers and domestic numbers, after concluding that each of the foreign telephone numbers satisfied the standard set forth in the Court's May 24, 2006 [Order] To summarize the alert system: every day new contacts are automatically revealed with the 3980 telephone numbers contained on the alert list described above, which themselves are present on the alert list either because they satisfied the reasonable articulable suspicion standard, or because they are domestic numbers that were either a FISC approved number or in direct contact with a number that did so."); *see also* Declaration of Lieutenant General Keith B. Alexander at 7, *In re* Prod. of Tangible Things from [REDACTED], No. BR 08-13 (FISA Ct. Feb. 13, 2009), available at http://www.dni.gov/files/documents/section/pub_Feb%2012%202009%20Memorandum%20of%20US.pdf, [<http://perma.cc/0TjRzWGeXcT>] (reprinting the same report text and stating, "in short, the reports filed with the Court incorrectly stated that the telephone identifiers on the alert list satisfied the RAS standard. In fact, the majority of telephone identifiers included on the alert list had not been RAS approved"). Note that No. BR 06-05 is the initial authorization of the telephony metadata program, May 24, 2006. No. BR-08 was a renewal application, filed Aug. 18, 2006. No. BR 08-13 is a subsequent authorization. The May 2006 order, however, has seven tabs for different docket numbers, all of which have been redacted, suggesting that there are other, related programs underway.

239. Memorandum of the United States in Response to the Court's Order Dated Jan. 28, 2009 at 17, *In re* Prod. of Tangible Things From [REDACTED], No. BR 08-13 (FISA Ct. Feb. 17, 2009), available at http://www.dni.gov/files/documents/section/pub_Feb%2012%202009%20Memorandum%20of%20US.pdf, [<http://perma.cc/0TjRzWGeXcT>]; Declaration of Lieutenant General Keith B. Alexander at 42, *In re* Prod. of Tangible Things From [REDACTED], No. BR 08-13 (FISA Ct. Feb. 13, 2009), available at http://www.dni.gov/files/documents/section/pub_Feb%2012%202009%20Memorandum%20of%20US.pdf, [<http://perma.cc/0TjRzWGeXcT>] (further noting that the 275 reports provided to the FBI tipped a total of 2549 telephone identifiers as being in contact with identifiers used to query the system).

from the automated alert process.²⁴⁰ In a careful use of language, the government noted, “NSA did not identify any report that resulted from the use of a non-RAS-approved ‘seed’ identifier.”²⁴¹ The government did not detail how complete the NSA had been in considering the reports; nor did it claim that none of the reports had resulted from non-RAS-approved identifiers.²⁴² The government also did not address the dissemination of metadata reports within NSA and subsequent actions that resulted from the process.

Despite the gross violation of FISC’s order, the government argued that FISC should neither rescind nor modify its order.²⁴³ As required by FISC, the NSA had undertaken an end-to-end system engineering and process review (technical and operational) of its handling of business records metadata; it had undertaken a review of domestic identifiers to ensure that they are RAS-compliant; and it had undertaken an audit of all queries made of the business records metadata repository since November 1, 2008 with the purpose of determining if any queries had been made using non-RAS-approved identifiers.²⁴⁴ The NSA had again trained its employees and adopted new technologies to limit the number of “hops” permitted from an RAS-

240. Memorandum of the United States in Response to the Court’s Order Dated Jan. 28, 2009 at 17, *In re Prod. of Tangible Things From [REDACTED]*, No. BR 08-13 (FISA Ct. Feb. 17, 2009), available at http://www.dni.gov/files/documents/section/pub_Feb%2012%202009%20Memorandum%20of%20US.pdf, [<http://perma.cc/0TjRzWGeXcT>].

241. *Id.*

242. See Declaration of Lieutenant General Keith B. Alexander at 36–37, *In re Prod. of Tangible Things From [REDACTED]*, No. BR 08-13 (FISA Ct. Feb. 13, 2009), available at http://www.dni.gov/files/documents/section/pub_Feb%2012%202009%20Memorandum%20of%20US.pdf, [<http://perma.cc/0TjRzWGeXcT>] (“[The NSA] has . . . conducted a review of all 275 reports of domestic contacts NSA has disseminated as result of contact chaining [REDACTED] of the NSA’s Archive of BR FISA material. NSA has identified no report that resulted from the use of a non-RAS approved identifier as the initial seed identifier for chaining through the BR FISA material.” (internal footnotes omitted)).

243. Memorandum of the United States in Response to the Court’s Order Dated Jan. 28, 2009 at 2, 15–21, *In re Production of Tangible Things From [REDACTED]*, No. BR 08-13 (FISA Ct. Feb. 17, 2009), available at http://www.dni.gov/files/documents/section/pub_Feb%2012%202009%20Memorandum%20of%20US.pdf, [<http://perma.cc/0TjRzWGeXcT>].

244. *Id.* at 19.

approved seed identifier to three.²⁴⁵ The government offered to take additional steps to avoid having the program shut down, all of which amounted to involving DOJ's National Security Division more deeply in the telephony metadata program.²⁴⁶

b. Further Noncompliance

Although the January 2009 incident represents the first admission of noncompliance that was made public, it is far from the first—or only—time that the NSA acted outside the scope of its authority to collect records under section 215 of the USA PATRIOT Act.²⁴⁷ Recently released documents provide myriad further examples.

In September 2006, for instance, the NSA's Inspector General expressed concern that the agency was collecting more data than authorized under the order.²⁴⁸ The NSA had been obtaining 16-digit credit card numbers as well as names or partial names contained in the records of operator-assisted calls.²⁴⁹ It

245. *Id.* at 20.

246. *See id.* at 20–21 (listing under “Additional Oversight Mechanisms the government Will Implement”: (1) NSA's OGC consulting with DOJ's National Security Division (NSD) on “all significant legal opinions that relate the interpretation, scope and/or implementation” of FISC orders related to BR 08-13; (2) NSA's OGC providing NSD with copies of the mandatory procedures; (3) NSA's OGC promptly providing NSD with copies of all formal briefing and/or training materials; (4) arranging meetings among NSA's OGC, NSD, and NSA's Director of Signals Intelligence prior to seeking renewal of the orders; (5) meetings once per period of future orders between NSA's OIG and NSD; (6) review and approval of all proposed automated query processes prior to implementation).

247. *See, e.g.*, Memorandum of the United States in Response to the Court's Order Dated Jan. 28, 2009 at 19, *In re* Production of Tangible Things From [REDACTED], No. BR 08-13, available at http://www.dni.gov/files/documents/section/pub_Feb%2012%202009%20Memorandum%20of%20US.pdf, [<http://perma.cc/0TjRzWGeXcT>] (citing notice of compliance filed Jan. 26, 2009, which reports that between Dec. 10, 2008, and Jan. 23, 2009, two analysts conducted 280 queries using non-RAS-approved identifiers).

248. *See* OFFICE OF THE INSPECTOR GEN., *supra* note 1, at 2–3 (see page 95–96 of 1846 and 1862 Production, Mar. 5, 2009) (“[M]anagement controls do not provide reasonable assurance that NSA will comply with the following terms of the Order: ‘NSA may obtain telephony metadata, which includes comprehensive communications, routing information, including but not limited to session identifying information, trunk identifier, and time and duration of a call. Telephony metadata does not include the substantive content of any communications, or the name, address, or financial information of a subscriber or customer.’”).

249. *See id.* at 3 (see page 96 of 1846 and 1862 Production, Mar. 5, 2009).

later emerged that an over-collection filter inserted in July 2008 failed to function.²⁵⁰

On October 17, 2008, the government reported to FISC that, after FISC authorized the NSA to increase the number of analysts working with the business records metadata, and had directed that the NSA train the newly-authorized analysts, thirty-one (out of eighty-five) analysts subsequently queried the business records metadata in April 2008 *without even being aware that they were doing so*.²⁵¹ The upshot was that NSA analysts used 2373 foreign telephone identifiers to query the business records metadata without first establishing reasonable, articulable suspicion.²⁵² Despite taking corrective steps, on December 11, 2008, the government notified FISC that an analyst had not installed a modified access tool and, resultantly, had again queried the data using five identifiers for which no RAS standard had been satisfied.²⁵³

Just over a month later, the government informed FISC that, between December 10, 2008 and January 23, 2009, two analysts had used 280 foreign telephone identifiers to query the business records metadata without first establishing RAS.²⁵⁴

The process initiated in January 2009 identified additional incidents where the NSA had failed to comply with FISC's orders.²⁵⁵ In February 2009, the NSA brought two further matters

250. *In re* Production of Tangible Things from [REDACTED], Order, No. BR 08-13, at 17 (FISA Ct. Mar. 2, 2009), available at http://www.dni.gov/files/documents/section/pub_March%202009%20Order%20from%20FISC.pdf, [<http://perma.cc/0FW9D1bPVUv>] (citing Government's Response to the Court's Order of Jan. 16, 2009, at 13).

251. *Id.* at 9.

252. *Id.*

253. *Id.* at 10 (citing Preliminary Notice of Compliance Incident at 2, No. BR 08-08 (FISA Ct. Dec. 11, 2008)).

254. *Id.* (citing Notice of Compliance Incident at 2, No. BR 08-13 (FISA Ct. Jan. 26, 2009)).

255. Memorandum of the United States in Response to the Court's Order Dated Jan. 28, 2009 at 6, *In re* Prod. of Tangible Things from [REDACTED], No. BR 08-13 (FISA Ct. Feb. 17, 2009), available at http://www.dni.gov/files/documents/section/pub_Feb%2012%202009%20Memorandum%20of%20US.pdf, [<http://perma.cc/0TjRzWGeXcT>]; see also Press Release, Office of the Dir. of Nat'l Intelligence, DNI Clapper Declassifies Intelligence Community Documents Regarding Collection Under Section 501 of the Foreign Intelligence Surveillance Act (FISA) (Sept. 10, 2013), available at <http://www.dni.gov/index.php/newsroom/press-releases/191-press-releases-2013/927-draft-document>, [<http://perma.cc/0B43x9pG7Go>]; SECTION 215 WHITE PAPER, *supra*

to FISC's attention. The first centered on the NSA's use of one of its analytical tools to query the business records metadata, using non-RAS-approved telephone numbers.²⁵⁶ This tool had been used since FISC's initial order in May 2006 to search both the business records metadata and other NSA databases.²⁵⁷ Also in February 2009, the NSA notified DOJ's National Security Division that the NSA's audit had identified three analysts who conducted chaining on the business records metadata using fourteen telephone identifiers that had not been RAS-approved before the queries.²⁵⁸

In May 2009, two additional compliance issues arose.²⁵⁹ The first compliance incident is completely redacted. The second notes a dissemination-related problem: that the unminimized results of some queries of metadata had been "uploaded [by the NSA] into a database to which other intelligence agencies . . . had access."²⁶⁰ According to the government, providing other agencies access to this information may have resulted in

note 2, at 5 ("Since the telephony metadata collection program under Section 215 was initiated, there have been a number of significant compliance and implementation issues that were discovered The incidents, and the Court's responses, were . . . reported to the Intelligence and Judiciary Committees in great detail.").

256. Notice of Compliance Incidents at 2, *In re* Production of Tangible Things from [REDACTED], No. BR 08-13 (FISA Ct. Feb. 26, 2009), available at http://www.dni.gov/files/documents/section/pub_Feb%2026%202009%20Notification%20of%20Compliance%20Incident.pdf, [http://perma.cc/KQ87-TM6B].

257. *Id.* at 3.

258. According to Keith Alexander's Supplemental Declaration, one analyst conducted contact chaining queries on four non-RAS-approved telephone identifiers on November 5, 2008; a second analyst conducted one contact chaining query on one non-RAS-approved telephone identifier on November 18, 2008; and a third analyst conducted contact chaining queries on three non-RAS-approved telephone identifiers on December 31, 2008; one non-RAS approved identifier on January 5, 2009; three non-RAS approved identifiers on January 15, 2009; and two non-RAS approved identifiers on January 22, 2009. Supplemental Declaration of Lieutenant General Keith B. Alexander at 8, *In re* Production of Tangible Things, No. BR 08-13 (FISA Ct. Feb. 25, 2009), available at http://www.dni.gov/files/documents/section/pub_Feb%2026%202009%20Notification%20of%20Compliance%20Incident.pdf, [http://perma.cc/J79T-T3VD].

259. *In re* Application of the Federal Bureau of Investigation for an Order Requiring the Prod. of Tangible Things From [REDACTED], Order, No. BR 09-06, at 4 (FISA Ct. June 22, 2009), available at http://www.dni.gov/files/documents/section/pub_Jun%2022%202009%20Order.pdf, [http://perma.cc/0D4dE8vvr98] (referencing government responses to the court's May 29, 2009 Supplemental Order).

260. *Id.* at 5 (quoting Preliminary Notice of Compliance Incident at 2, No. BR 09-06 (FISA Ct. June 16, 2009)).

the dissemination of U.S. person information in violation of both U.S. Signals Intelligence Directive 18 as well as the more restrictive conditions FISC imposed in BR 09-06.²⁶¹

c. FISC Response

Repeatedly, instead of rescinding prior collection programs, FISC merely imposed further requirements on the government.²⁶² By spring of 2009, FISC had become fed up with the NSA—yet, not fed up enough to actually halt the program. Instead, it insisted on two procedures designed to give FISC greater insight into how the NSA was using and distributing information related to the telephony metadata: that the NSA return to FISC before each query of the database, and that the NSA file weekly reports with FISC detailing any dissemination of the information. Both protections proved temporary.

FISC's first temporary solution was to require what traditional FISA actually required: NSA application to FISC prior to targeting. Between institution of the review and the final report, FISC required the NSA to seek approval to query the database on a case-by-case basis. FISC was particularly concerned that the NSA had averred that having access to all call detail records

“is vital to NSA's counterterrorism intelligence mission” because “[t]he only effective means by which NSA analysts are able continuously to keep track of [REDACTED] and all affiliates of one of the aforementioned entities [who are taking steps to disguise and obscure their communications and

261. *Id.*

262. The government cites multiple other cases, with key information redacted as follows: “[REDACTED] Primary Order, docket number [REDACTED] at 11-12 (requiring, in response to an incident of noncompliance, NSA to file with the Court every thirty days a report discussing, among other things, queries made since the last report to the Court and NSA's application of the relevant standard); *see also* [REDACTED] docket numbers [REDACTED] (prohibiting the querying of data using “seed” accounts validated using particular information).” Memorandum of the United States in Response to the Court's Order Dated Jan. 28, 2009 at 16, *In re* Prod. of Tangible Things From [REDACTED], No. BR 08-13 (FISA Ct. Feb. 17, 2009), available at http://www.dni.gov/files/documents/section/pub_Feb%2012%202009%20Memorandum%20of%20US.pdf, [<http://perma.cc/0TjRzWGeXcT>].

identities], is to obtain and maintain an archive of metadata that will permit these tactics to be uncovered.²⁶³

According to FISC, the NSA had also suggested that:

To be able to exploit metadata fully, the data must be collected in bulk The ability to accumulate a metadata archive and set it aside for carefully controlled searches and analysis will substantially increase NSA's ability to detect and identify members of [REDACTED].²⁶⁴

Because the order being sought meant, if granted, that the NSA would be collecting call detail records of U.S. persons located within the United States, who were not themselves the target of any FBI investigation and whose metadata could not otherwise be legally obtained in bulk, FISC had adopted minimization procedures. It had required, *inter alia*, that:

[A]ccess to the archived data shall occur only when NSA has identified a known telephone identifier for which, based on the factual and practical considerations of everyday life on which reasonable and prudent persons act, there are facts giving rise to a reasonable, articulable suspicion that the telephone identifier is associated with [REDACTED].²⁶⁵

FISC had a difficult time believing the NSA's claim that its non-compliance with FISC's orders resulted from NSA personnel believing that FISC's restrictions on access to the business records metadata only applied to "archived data" (that is, data located in certain databases). "That interpretation of [FISC's] Orders," Judge Reggie Walton wrote, "strains credulity."²⁶⁶ The NSA had compounded its bad behavior by repeatedly submitting inaccurate

263. *In re* Production of Tangible Things from [REDACTED], Order, No. BR 08-13, at 2 (FISA Ct. Mar. 2, 2009) (quoting Application Exhibit A, Declaration of [REDACTED], Signals Intelligence Directorate Deputy Program Manager [REDACTED], NSA at 5, *In re* Production of Tangible Things from [REDACTED], No. BR 08-13 (FISA Ct. Dec. 11, 2008)), available at http://www.dni.gov/files/documents/section/pub_March%20202009%20Order%20from%20FISC.pdf, [<http://perma.cc/BP9D-DUUL>].

264. *Id.* (quoting Application Exhibit A, Declaration of [REDACTED], Signals Intelligence Directorate Deputy Program Manager [REDACTED], NSA at 5-6, *In re* Production of Tangible Things from [REDACTED], No. BR 08-13).

265. *Id.* at 3 (emphasis omitted) (quoting *In re* Production of Tangible Things from [REDACTED], Primary Order, No. BR 08-13, at 8 (FISA Ct. Dec. 11, 2008)).

266. *Id.* at 5.

descriptions of how it developed and used the alert list process.²⁶⁷ In support of its claim that the program was vital for U.S. national security, the NSA had offered as evidence the paltry claim that, after nearly three years of sweeping up all telephony metadata, the NSA had generated 275 domestic security reports that, in turn, had spurred three preliminary investigations.²⁶⁸

FISC objected to the government's assertion that FISC "need not take any further remedial action."²⁶⁹ FISC has also noted that, until the NSA has completed the review, "[FISC] sees little reason to believe that the most recent discovery of a systemic, ongoing violation—on February 18, 2009—will be the last."²⁷⁰ Accordingly, starting in March 2009, though the NSA could continue to collect data and to test the telephony metadata system, it would only be allowed to query it with a FISC order—or, in an emergency, to query the database and then to inform FISC by 5:00 PM, Eastern Time, on the next business day.²⁷¹ In September 2009, however, FISC lifted the requirement for the NSA to seek approval in every case.²⁷²

The second protection FISC introduced was, starting on July 3, 2009, to require the NSA to file a weekly report with FISC, listing each time, over the seven-day period ending the previous Friday, in which the NSA had shared, "in any form, information obtained or derived from the [REDACTED] BR metadata collec-

267. *Id.* at 6.

268. *Id.* at 13 ("[T]he mere commencement of a preliminary investigation, by itself, does not seem particularly significant . . . The time has come for the government to describe to the Court how, based on the information collected and analyzed during [the duration of the program], the value of the program to the nation's security justifies the continued collection and retention of massive quantities of U.S. person information.").

269. *Id.* at 14 (quoting Notice of Compliance Incident at 6, *In re* Production of Tangible Things from [REDACTED], No. BR 08-13 (FISA Ct. Feb. 26, 2009)).

270. *Id.* at 16.

271. *Id.* at 18–19.

272. See Press Release, Office of the Dir. of Nat'l Intelligence, DNI Clapper Declassifies Intelligence Community Documents Regarding Collection Under Section 501 of the Foreign Intelligence Surveillance Act (FISA) (Sept. 10, 2013), available at <http://www.dni.gov/index.php/newsroom/press-releases/191-press-releases-2013/927-draft-document>, [<http://perma.cc/0B43x9pG7Go>].

tions with anyone outside NSA.”²⁷³ Again, consistent with traditional FISA, FISC added special protections for U.S. persons:

For each such instance, the government shall specify the date on which the information was shared, the recipient of the information, and the form in which the information was communicated (e.g., written report, email, oral communication, etc.). For each such instance in which U.S. person information has been shared, the Chief of Information Sharing of NSA’s Signals Intelligence Directorate shall certify that such official determined, prior to dissemination, the information to be related to counterterrorism information and necessary to understand the counterterrorism information or to assess its importance.²⁷⁴

In August 2009, the government submitted its end-to-end assessment of the NSA telephony metadata system.²⁷⁵ FISC lifted its requirements, leaving future dissemination decisions up to the NSA. Whether the requirements with which the NSA was left effectively check the exercise of authorities is questionable. Before the dissemination of information of U.S. persons’ information outside the Agency, an NSA official must determine that the information is “related to counterterrorism information and is necessary to understand the counterterrorism information or assess its importance.”²⁷⁶ Because the government already considers all of the information in the database to be relevant to counterterrorism investigations, and has already argued to FISC (and FISC has agreed), that the collection of such data is necessary to understand its counterterrorism information, the degree to which this restriction really prevents such dissemination is open to question.

273. *In re* Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things from [REDACTED], Order, No. BR 09-06, at 7 (FISA Ct. June 22, 2009), available at http://www.dni.gov/files/documents/section/pub_Jun%2022%202009%20Order.pdf, [<http://perma.cc/0Ur433saA6q>].

274. *Id.*

275. Report of the United States, *In re* Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things from [REDACTED], No. BR 09-09 (FISA Ct. Aug. 13, 2009), available at http://www.dni.gov/files/documents/section/pub_August%2019%202009%20Report%20of%20the%20US%20with%20Attachments%2020130910.pdf, [<http://perma.cc/0j3hGV41doz>].

276. SECTION 215 WHITE PAPER, *supra* note 2, at 5.

d. Technological Gap

A critical part of FISC's failure to provide effective oversight of the process relates to FISC's decision to have the NSA perform the targeting decision. Part of the problem also stems from FISC's discomfort with the technological aspects of the collection and analysis of digital information. For much of the discussion of noncompliance incidents, for instance, it appears that neither the NSA nor FISC had an adequate understanding of how the algorithms operate. Nor did they understand the type of information that had been incorporated into different databases, and whether they had been subjected to the appropriate legal analysis before data mining.

A similar problem may accompany the reporting requirements to Congress. In March 2009, for example, the DOJ submitted several FISC opinions and government filings—relating to the discovery and remediation of compliance incidents in its handling of bulk telephony metadata—to the Chairmen of the Intelligence and Judiciary Committees.²⁷⁷ A subsequent letter noted that the House and Senate Intelligence and Judiciary Committees had received briefings in March, April, and August before receiving a copy of the NSA's review in September 2009.²⁷⁸ To the extent that the representations of the agency are

277. Letter from M. Faith Burton, Acting Assistant Attorney Gen., to the Hon. Patrick J. Leahy, Chairman, Comm. on the Judiciary, U.S. Senate; the Hon. Dianne Feinstein, Chairman, Select Comm. on Intelligence, U.S. Senate; the Hon. John Conyers, Jr., Chairman, Comm. on the Judiciary, U.S. House of Representatives; the Hon. Silvestre Reyes, Chairman, Permanent Select Comm. on Intelligence, U.S. House of Representatives (Mar. 5, 2009), *available at* http://www.dni.gov/files/documents/section/pub_Mar%205%202009%20Cover%20Letter%20to%20Chairman%20of%20Intel%20and%20Judiciary%20Committees.pdf, [<http://perma.cc/TEN8-VUZG>].

278. Press Release, Office of the Dir. of Nat'l Intelligence, DNI Clapper Declassifies Intelligence Community Documents Regarding Collection Under Section 501 of the Foreign Intelligence Surveillance Act (FISA) (Sept. 10, 2013), *available at* <http://icontherecord.tumblr.com/>, [<http://perma.cc/0B43x9pG7Go>]; Letter from Ronald Weich, Assistant Attorney Gen., to the Hon. Patrick J. Leahy, Chairman, Comm. on the Judiciary, U.S. Senate; the Hon. Dianne Feinstein, Chairman, Select Comm. on Intelligence, U.S. Senate; the Hon. John Conyers, Jr., Chairman, Comm. on the Judiciary, U.S. House of Representatives; the Hon. Silvestre Reyes, Chairman, Permanent Select Comm. on Intelligence, U.S. House of Representatives (Sept. 3, 2009), *available at* http://www.dni.gov/files/documents/section/pub_Sep%203%202009%20Cover%20letter%20to%20Chairman%20of%20the%20Intelligence%20and%20Judiciary%20Committees.pdf, [<http://perma.cc/09KwyBTiXcp>].

heavily dependent on technical knowledge, the implications may not be readily apparent to lawmakers.

2. *Issuance of Detailed Legal Reasoning and Creation of Precedent*

To enforce the specialized probable cause standard encapsulated in FISA, Congress created a court of specialized but exclusive jurisdiction.²⁷⁹ Its job was to ascertain whether sufficient probable cause existed for a target to be considered a foreign power, or an agent thereof; whether the applicant had provided the necessary details for the surveillance; and whether the appropriate certifications and findings had been made.

It is thus surprising that the government considers these orders now to be evidence of precedent, on the basis of which, it argues, the programs are legal. In *ACLU v. Clapper*,²⁸⁰ for instance, the government responded to the argument that it had exceeded its statutory authority under FISA by arguing:

[S]ince May 2006, fourteen separate judges of the FISC have concluded on thirty-four occasions that the FBI satisfied this requirement, finding “reasonable grounds to believe” that the telephony metadata sought by the Government “are relevant to authorized investigations . . . being conducted by the FBI . . . to protect against international terrorism.”²⁸¹

The government went on to cite Judge Eagan’s August 2013 memorandum opinion in further support of its interpretation of “relevance.”²⁸² These were the only points of reference that mattered: “Considering that the Government has consistently demonstrated the relevance of the requested records to the FISC’s satisfaction, as Section 215 requires, it is difficult to understand how the government can be said to have acted in excess of statutory authority.”²⁸³

279. Theodore W. Ruger, *Chief Justice Rehnquist’s Appointments to the FISA Court: An Empirical Perspective*, 101 NW. U. L. REV. 239, 244 (2007).

280. 959 F. Supp. 2d 724 (S.D.N.Y. 2013).

281. Defendants’ Memorandum of Law in Opposition to Plaintiffs’ Motion for a Preliminary Injunction at 16, *Clapper*, 959 F. Supp. 2d 724, available at https://www.aclu.org/files/assets/2013.10.01_govt_oppn_to_pi_motion.pdf, [http://perma.cc/0KsuWbyJspP].

282. *Id.*

283. *Id.*

Even more surprising than the role the granting of orders is playing for establishing legal precedent is the revelation that FISC has greatly broadened the “special needs” exception to the Fourth Amendment to embrace wholesale data collection.²⁸⁴ Although the Supreme Court has never recognized such an exception, FISC’s unique constitutional interpretation has served to authorize broad collection of information on U.S. citizens. Notably, because of the secret nature of FISC’s proceedings and the ex parte nature of the court, there are no advocates who could appeal a decision based on this interpretation to the Supreme Court. Consequently, an unreviewable, complex body of law, establishing doctrines unrecognized by the Supreme Court, has emerged as precedent for future application to FISC.

In *In re Directives*, FISC looked back at its decision in *In re Sealed Case* to confirm “the existence of a foreign intelligence exception to the warrant requirement.”²⁸⁵ It acknowledged that FISC had “avoided an express holding that a foreign intelligence exception exists by assuming arguendo that whether or not the warrant requirements were met, the statute could survive on reasonableness grounds.”²⁸⁶ FISC went on to determine that, as a federal appellate court, it would “review findings of fact for clear error and legal conclusions (including determinations about the ultimate constitutionality of government searches or seizures) de novo.”²⁸⁷ It then asserted, for the first time, a foreign intelligence surveillance exception to the Fourth Amendment:

The question . . . is whether the reasoning of the special needs cases applies by analogy to justify a foreign intelligence exception to the warrant requirement for surveillance undertaken for national security purposes and directed at a foreign power or an agent of a foreign power reasonably believed to be located outside the United States. Applying principles derived from the special needs cases, we conclude

284. See Eric Lichtblau, *In Secret, Court Vastly Broadens Powers of N.S.A.*, N.Y. TIMES, July 7, 2013, at A1.

285. *In re Directives* [REDACTED] Pursuant to Section 105B of the Foreign Intelligence Surveillance Act, 551 F.3d 1004, 1010 (FISA Ct. Rev. 2008).

286. *Id.*

287. *Id.* at 1009.

that this type of foreign intelligence surveillance possesses characteristics that qualify it for such an exception.²⁸⁸

The court analogized the exception to the 1989 Supreme Court consideration of the warrantless drug testing of railway workers, on the grounds that the government's need to respond to an overriding public danger could justify a minimal intrusion on privacy.²⁸⁹ The government subsequently cited *In re Directives* in its August 9, 2013 white paper, defending the telephony metadata program, in support of an exception to the Fourth Amendment warrant requirement.²⁹⁰

FISC continues to go beyond its mandate. In August 2013, for instance, FISC issued a twenty-nine-page Amended Memorandum Opinion regarding the FBI's July 18, 2013 application for the telephony metadata program.²⁹¹ Appending the seventeen-page order to the opinion, Judge Claire V. Eagan considered Fourth Amendment jurisprudence, the statutory language of Section 215, and the canons of statutory construction to justify granting the order.²⁹² Similarly, in a 2002 per curiam opinion, FISC suggested the case raised "important questions of statutory interpretation, and constitutionality" and concluded "that FISA, as amended by the Patriot Act, supports the government's position, and that the restrictions imposed by the FISA court are not required by FISA or the Constitution."²⁹³

Congress did not design the Foreign Intelligence Surveillance Court or the Court of Review to develop its own jurisprudence. Particularly in light of the secrecy and lack of adversarial process inherent in the court, it is concerning that FISC's decisions have taken on a force of their own in legitimizing the collection of information on U.S. citizens.

288. *Id.* at 1011.

289. *Id.* at 1010–11.

290. SECTION 215 WHITE PAPER, *supra* note 2, at 15.

291. *In re* Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things from [REDACTED], No. BR 13-109 (FISA Ct. 2013), available at <http://www.uscourts.gov/uscourts/courts/fisc/br13-09-primary-order.pdf>, [<http://perma.cc/0LkgNZzvbBu>].

292. *Id.* at 28–29.

293. *In re* Sealed Case, 310 F.3d 717, 719–20 (FISA Ct. Rev. 2002).

3. *Judicial Design*

As mentioned above, Congress tried to construct an even-handed, neutral arbiter by requiring that (a) FISC judges be selected by the Chief Justice of the Supreme Court from at least seven different federal districts; (b) the judges serve staggered terms of up to seven years; and (c) having once served, such judges are ineligible for further service.²⁹⁴ To ensure diversity, any federal district court judge (including a senior judge), who has not previously served on FISC, may be selected.²⁹⁵ FISCR, in turn, is comprised of judges selected by the Chief Justice.²⁹⁶

This system has been called into question on two grounds: first, the lack of diversity regarding judicial appointment and, second, the high rate of applications being granted by FISC. Given these characteristics, critics question how effectively FISC operates as a check on the executive branch. The observations are important, but, without more information, it is difficult to determine the extent to which the current state of affairs has substantively impacted the process.

a. Appointments

To the extent that political ideology is reflected in the appointments process, the court is heavily weighted toward one side of the political spectrum. The past two Chief Justices have been appointed by Republican presidents, and they have tended to select judges that have been nominated by Republican administrations.²⁹⁷ Only one of the current eleven judges serving on FISC is a Democratic nominee. Over the past decade, of the twenty judges appointed to FISC and FISCR, only three have been Democratic nominees.

Although this raises questions about the even-handedness of the FISC appointments process, it would be premature to draw substantive conclusions based solely on the political makeup of the bench. Any meaningful examination of how composition influences the outcome of cases would need to compare either FISC decisions with other, more diverse courts, or the individual

294. 50 U.S.C. § 1803(a)(1), (d) (2006 & Supp. V 2011).

295. *Id.* at § 1803(a).

296. *Id.* at § 1803(b).

297. *See infra* Figure 1.

decisions reached by FISC judges appointed by one party with decisions reached by judges appointed by the opposing party.

Such studies would be almost impossible to conduct. FISC opinions are classified. Beyond this, they are *sui generis*, in that FISC is the only court that considers FISA applications. It also may be that externalities influence which judges opt for FISC membership. That is, more Republican appointees than Democratic appointees may inquire or make clear that they would be interested in serving on FISC. No studies have yet been conducted demonstrating why the appointments process aligns with political party, making any conclusions as to the effect somewhat arbitrary.

To the extent that political ideology enters into the equation, the way in which it has interacted with the court's role in establishing precedent deserves notice, as it undermines the appearance of a neutral arbiter and emphasizes deference to and support for greater power for the executive. According to the public record, FISCR, for instance, has only met twice: once in 2002 and once in 2008.²⁹⁸ On both occasions, the panels consisted entirely of Republican appointees, some of whom had publicly argued that FISA was an unconstitutional usurpation of executive power.

Judge Laurence Silberman of the D.C. Circuit testified to Congress in 1978 (when FISA was being debated) that the legislation violated the Constitution.²⁹⁹ Judge Silberman, who had previously served as Deputy Attorney General, was "absolutely convinced that the administration bill, if passed, would be an enormous and fundamental mistake which the Congress and the American people would have reason to regret."³⁰⁰ For Judge Silberman, the judiciary's role in any national security electronic surveillance should be circumscribed. He explained:

298. See *In re Directives* [REDACTED] Pursuant to Section 105B of Foreign Intelligence Surveillance Act, 551 F.3d 1004 (FISA. Ct. Rev. 2008); *In re Sealed Case*, 310 F.3d 717.

299. See *Foreign Intelligence Electronic Surveillance: Hearings on H.R. 5794, H.R. 9745, H.R. 7308, and H.R. 5632 Before the Subcomm. on Legislation of the H. Permanent Select Comm. on Intelligence*, 95th Cong. 221 (1978) (statement of the Hon. Laurence H. Silberman), available at <http://www.cnss.org/pages/foreign-intelligence-surveillance-act-fisa.html>, [<http://perma.cc/8EMD-ZGLW>].

300. *Id.* at 217.

I find the notion that the President’s constitutional authority to conduct foreign affairs and to command the armed forces precludes congressional intervention into the manner by which the executive branch gathers intelligence, by electronic or other means, to be unpersuasive, and in that respect I agree with my colleague here to the left. But to concede the propriety of a congressional role in this matter is by no means—and this is the burden of my testimony—to concede the propriety or constitutionality of the judicial role created by the administration’s bill.³⁰¹

The Judge’s chief concern was not a so-called “imperial presidency,” but the advent of an “imperial judiciary.”³⁰² The authorities transferred to FISC thus represented an unconstitutional erosion of executive power.³⁰³ Another FISC judge, Ralph Guy, similarly argued for the government as a U.S. Attorney in *United States v. United States District Court*³⁰⁴ that the President did not need a warrant to engage in national security surveillance.³⁰⁵ Along with Judge Leavy, a Reagan appointee, Judges Silberman and Guy heard the first appeal in the history of FISA—issuing a decision that made it possible for the government to use the looser restrictions in FISA even in cases in which the primary purpose of the investigation was criminal in nature.³⁰⁶

With the court overwhelmingly constituted by nominees of one political party, it is perhaps unsurprising that some of the most important decisions have been made by panels entirely constituted by the same. The FISCR panel that appears to have created a foreign intelligence exception to the Fourth Amendment warrant requirement lacked a diverse political base. It included Chief Judge Selya and Senior Circuit Judges Winter and Arnold—appointees of Presidents Ronald Reagan and George H. W. Bush.

To the extent that political appointments stand in as a proxy for political ideologies, such as greater deference to the executive branch, the lack of diversity in the appointments process—

301. *Id.* at 219.

302. *Id.*

303. *Id.*

304. 407 U.S. 297 (1972).

305. *See generally id.*

306. *See In re Sealed Case*, 310 F.3d 717, 736 (FISA Ct. Rev. 2002).

especially in regard to some of the most important and far-reaching secret decisions issued by the court—raises important questions about the extent to which FISC, as conceived by Congress, is serving as neutral arbiter. Without more detailed information about the judicial process, however, the extent to which this is the case remains in question.

FIGURE 1: JUDGES APPOINTED TO THE FOREIGN INTELLIGENCE SURVEILLANCE COURT AND COURT OF REVIEW BY ORIGINAL APPOINTMENT TO THE BENCH³⁰⁷

District Judge	Court	Dates of appointment	Appointing President
Rosemary M. Collyer*	FISC	3/8/2013–3/7/2020	George W. Bush
Claire Eagan*	FISC	2/13/2013–5/18/2019	George W. Bush
Michael W. Mosman*	FISC	5/4/2013–5/3/2020	George W. Bush
Raymond J. Dearie*	FISC	7/2/2012–7/1/2019	Ronald Reagan
William C. Bryson**	FISCR	12/1/2011–5/18/2018	Bill Clinton
Jennifer B. Coffman	FISC	5/19/2011–1/8/2013	Bill Clinton
F. Dennis Saylor IV*	FISC	5/19/2011–5/18/2018	George W. Bush
Martin L.C. Feldman*	FISC	5/19/2010–5/18/2017	Ronald Reagan
Susan W. Wright*	FISC	5/19/2009–5/18/2016	George H. W. Bush
Thomas F. Hogan*	FISC	5/19/2009–5/18/2016	Ronald Reagan
Morris S. Ar-	FISCR	6/13/2008–5/18/2015	George H.

307. See *Foreign Intelligence Surveillance Court, Foreign Intelligence Surveillance Court of Review: Current and Past Members*, FEDERATION AM. SCIENTISTS, <https://www.fas.org/irp/agency/doj/fisa/fisc-members.pdf>, [http://perma.cc/9FVC-XGMC] (last visited Dec. 2, 2013).

nold**			W. Bush
James B. Zagel*	FISC	5/19/2008–5/18/2015	Ronald Reagan
Mary A. McLaughlin*	FISC	5/19/2008–5/18/2015	Bill Clinton
Reggie Walton*	FISC	5/19/2007–5/18/2014	George W. Bush
Roger Vinson	FISC	5/4/2006–5/3/2013	Ronald Reagan
John D. Bates	FISC	2/22/2006–2/21/2013	George W. Bush
Bruce M. Selya	FISCR	5/19/2005–5/18/2012	Ronald Reagan
Malcolm Howard	FISC	5/19/2005–5/18/2012	Ronald Reagan
Frederick J. Scullin	FISC	5/19/2004–5/18/2011	Ronald Reagan
Dee Benson	FISC	4/8/2004–4/7/2011	George W. Bush
Ralph Winter	FISCR	11/14/2003–5/18/2010	Ronald Reagan
George P. Kazen	FISC	7/15/2003–5/18/2010	Jimmy Carter
Robert Broomfield	FISC	10/1/2002–5/18/2009	Ronald Reagan
Colleen Kollar-Kotelly	FISC	5/19/2002–5/18/2009	Bill Clinton
James G. Carr	FISC	5/19/2002–5/18/2008	Bill Clinton
James Robertson	FISC	5/19/2002–12/19/2005	Bill Clinton
John E. Conway	FISC	5/19/2002–10/30/2003	Ronald Reagan
Edward Leavy	FISCR	9/25/2001–5/18/2008	Ronald Reagan
Nathaniel M. Gorton	FISC	5/19/2001–5/18/2008	George W. Bush
Claude M. Hilton	FISC	5/18/2000–5/18/2007	Ronald Reagan

Michael J. Davis	FISC	5/18/1999–5/18/2006	Bill Clinton
Ralph B. Guy, Jr.	FISCR	10/8/1998–5/18/2005	Gerald Ford
Harold A. Baker	FISC	5/18/1998–5/18/2005	Jimmy Carter
Stanley S. Brotman	FISC	7/17/1997–5/18/2004	Gerald Ford
William H. Stafford	FISC	5/19/1996–5/18/2003	Gerald Ford
Royce C. Lamberth	FISC	5/19/1995–5/18/2002	Ronald Reagan
Laurence H. Silberman	FISCR	6/18/1996–5/18/2003	George W. Bush
Paul H. Roney	FISCR	9/13/1994–5/18/2001	Richard Nixon
John F. Keenan	FISC	7/27/1994–5/18/2001	Ronald Reagan
James C. Cacheris	FISC	9/10/1993–5/18/2000	Ronald Reagan
Earl H. Carroll	FISC	2/23/1993–5/18/1999	Jimmy Carter
Charles Schwartz Jr.	FISC	8/5/1992–5/18/1998	Gerald Ford
Bobby R. Baldock	FISCR	6/17/1992–5/18/1998	Ronald Reagan
Ralph G. Thompson	FISC	6/11/1990–5/18/1997	Gerald Ford
Frank H. Freedman	FISC	5/30/1990–5/18/1994	Richard Nixon
Wendell A. Miles	FISC	9/21/1989–5/18/1996	Richard Nixon
Robert W. Warren	FISCR	10/30/1989–5/18/1996	Richard Nixon
Sidney Aronovitz	FISC	6/8/1989–5/18/1992	Gerald Ford
Joyce H. Green	FISC	5/18/1988–5/18/1995	Jimmy Carter

Conrad K. Cyr	FISC	5/18/1987– 11/20/1989	Ronald Reagan
Collins J. Seitz	FISCR	3/19/1987–3/18/1994	Lyndon B. Johnson

* Denotes current members of FISC

**Denotes current members of FISCR

b. Order Rate

Augmenting concerns prompted by the lack of diversity in terms of appointments to FISC and FISCR is the rather notable success rate the government enjoys in its applications to the court. Scholars have noted that the success rate is “unparalleled in any other American court.”³⁰⁸ Over the first two and a half decades, for instance, FISC approved nearly every single application without any modification.³⁰⁹ Between 1979 and 2003, FISC denied only three out of 16,450 applications.³¹⁰

Since 2003, FISC has ruled on 18,473 applications for electronic surveillance and physical search (2003–2008), and electronic surveillance (2009–2012).³¹¹ Court supporters note that a significant number of these applications are either modified or withdrawn by the government prior to FISC ruling. But even here, the numbers are quite low: 493 modifications still only comes to 2.6% of the total number of applications. Simultaneously, the government has only withdrawn twenty-six applications prior to FISC ruling.³¹² These numbers speak to the presence of informal processes, whereby FISC appears to be influencing the contours of applications. Without more information about the types of modifications that are being required, however, it is impossible to

308. Ruger, *supra* note 266, at 245.

309. See 1 KRIS & WILSON, *supra* note 167, at 469; Letter from Attorney Gen. William French Smith to Dir., Admin. Office of the U.S. Courts (Apr. 22, 1981), available at <http://www.fas.org/irp/agency/doj/fisa/1980rept.html>, [<http://perma.cc/0gryFWv7hZe>] (“No orders were entered which modified or denied the requested authority, except one case in which the Court modified an order and authorized an activity for which court authority had not been requested.”).

310. LAURA K. DONOHUE, THE COST OF COUNTERTERRORISM: POWER, POLITICS, AND LIBERTY 232 (2008).

311. See *infra* Figure 2.

312. *Id.*

gauge either the level of oversight or the extent to which FISC is altering the applications.

Critics also point to the risk of capture presented by in camera, ex parte proceedings, and note that out of 18,473 rulings, FISC has only denied eight in whole and three in part. Whatever the substantive effect might be, the presentational impact is of note.

FIGURE 2: FISC RULINGS ON ELECTRONIC SURVEILLANCE AND PHYSICAL SEARCH (2003–2008) AND ELECTRONIC SURVEILLANCE (2009–2012)³¹³

Year	Applications on which FISC ruled	Approved	Modified	Denied in part	Denied in whole	Withdrawn by gov't
2003 ³¹⁴	1727	1724	79	0	3 ³¹⁵	0
2004 ³¹⁶	1756 ³¹⁷	1756	94	0	0	3
2005 ³¹⁸	2072 ³¹⁹	2072	61	0	0	2
2006 ³²⁰	2176 ³²¹	2176	73	1	0	5

313. Starting in 2009, the Department of Justice began providing the breakdown of the number approved, modified, denied in part, denied in whole, or withdrawn by the government prior to the FISC ruling only for those applications involving electronic communications. Prior to that time, these numbers were combined.

314. Letter from William E. Moschella, Assistant Attorney Gen., Office of Legislative Affairs, U.S. Department of Justice, to Mr. L. Ralph Mechem, Dir., Admin. Office of the United States Courts (Apr. 30, 2004), *available at* <https://www.fas.org/irp/agency/doj/fisa/2003rept.pdf>, [<http://perma.cc/0Vu9UXSTi4y>].

315. An additional application was initially denied but later approved. *Id.*

316. Letter from William E. Moschella, Assistant Attorney Gen., Office of Legislative Affairs, U.S. Department of Justice, to the Hon. J. Dennis Hastert, Speaker, U.S. House of Representatives (Apr. 1, 2005), *available at* <https://www.fas.org/irp/agency/doj/fisa/2004rept.pdf>, [<http://perma.cc/4W63-92U5>].

317. Of 1758 submitted, three were withdrawn prior to FISC ruling and one was resubmitted. *Id.*

318. Letter from William E. Moschella, Assistant Attorney Gen., Office of Legislative Affairs, U.S. Department of Justice, to the Hon. J. Dennis Hastert, Speaker, U.S. House of Representatives (Apr. 28, 2006), *available at* <https://www.fas.org/irp/agency/doj/fisa/2005rept.pdf>, [<http://perma.cc/UV22-GC3G>].

319. Of 2074 submitted, two were withdrawn prior to FISC ruling, and one was resubmitted. *Id.*

320. Letter from William E. Moschella, Assistant Attorney Gen., Office of Legislative Affairs, U.S. Department of Justice, to the Hon. Nancy Pelosi, Speaker, U.S. House of Representatives (Apr. 27, 2007), *available at* <https://www.fas.org/irp/agency/doj/fisa/2006rept.pdf>, [<http://perma.cc/32AX-FEYA>].

321. Of 2181 submitted, five were withdrawn prior to FISC ruling. *Id.*

2007 ³²²	2371	2370	86	1	3 ³²³	0
2008 ³²⁴	2082	2083 ³²⁵	2	0	1	0
2009 ³²⁶	1321 ³²⁷	1320	14	1	1	8
2010 ³²⁸	1506 ³²⁹	1506	14	0	0	5
2011 ³³⁰	1674 ³³¹	1674	30	0	0	2

322. Letter from Brian A. Benczkowski, Principal Deputy Assistant Attorney Gen., Office of Legislative Affairs, U.S. Department of Justice, to the Hon. Nancy Pelosi, Speaker, U.S. House of Representatives (Apr. 30, 2008), *available at* <https://www.fas.org/irp/agency/doj/fisa/2007rept.pdf>, [http://perma.cc/NTD6-7CJ4].

323. Discrepancy in the numbers stems in part from holdover applications and denials. Two applications, for instance, filed in 2006 were not approved until 2007. *Id.*

324. Letter from Ronald Weich, Assistant Attorney Gen., Office of Legislative Affairs, U.S. Department of Justice, to the Hon. Harry Reid, Majority Leader, U.S. Senate (May 14, 2009), *available at* <https://www.fas.org/irp/agency/doj/fisa/2008rept.pdf>, [http://perma.cc/8KA4-E9UC].

325. Discrepancy in the numbers stems in part from holdover applications and denials. Two applications filed in CY 2007 were not approved until CY 2008. *Id.*

326. Letter from Ronald Weich, Assistant Attorney Gen., Office of Legislative Affairs, U.S. Department of Justice, to the Hon. Joseph R. Biden, Jr., President, U.S. Senate (Apr. 30, 2010), *available at* <https://www.fas.org/irp/agency/doj/fisa/2009rept.pdf>, [http://perma.cc/5VA5-8R6B].

327. For the first time since 2003, no numbers are available for modifications or denials for the full number of applications submitted (physical search, electronic surveillance, and combined applications). Instead, the report notes that of the 1376 total submitted in the former three categories, 1329 were related to electronic surveillance. Eight of these applications were withdrawn, one denied in whole, one denied in part, and fourteen modified, with 1320 approved. The number of applications is thus missing the numbers for physical search and physical search combined applications. *Id.*

328. Letter from Ronald Weich, Assistant Attorney Gen., Office of Legislative Affairs, U.S. Department of Justice, to the Hon. Harry Reid, Majority Leader, U.S. Senate (Apr. 29, 2011), *available at* <https://www.fas.org/irp/agency/doj/fisa/2010rept.pdf>, [http://perma.cc/G36L-LBED].

329. The total number of electronic surveillance, physical search, and combined applications was 1579. The report, however, isolates the electronic applications (1511), and provides breakdowns for modifications, denials, etc., for just that category. Of the total of 1511, five were withdrawn by the government prior to FISC ruling. *Id.*

330. Letter from Ronald Weich, Assistant Attorney Gen., Office of Legislative Affairs, U.S. Department of Justice, to the Hon. Joseph R. Biden, Jr., President, U.S. Senate (Apr. 30, 2012), *available at* <https://www.fas.org/irp/agency/doj/fisa/2011rept.pdf>, [http://perma.cc/HD44-EAY5].

331. Note that there were 1745 total applications that included electronic surveillance and physical searches for foreign intelligence purposes. It appears that approximately seventy of the orders related solely to physical search, as the breakdown for electronic surveillance is only done for the 1674. Two of the initial orders were withdrawn prior to FISC ruling. *Id.*

2012 ³³²	1788 ³³³	1788	40	0	0	1
Totals	18,473	18,469	493	3	8	26

Setting modifications aside for the moment, the deference that appears to exist regarding outright denials or granting of orders seems to extend to FISC rulings with regard to business records. Almost no attention, however, has been paid to this area. It appears that FISC has *never* denied an application for an order under this section. That is, of 751 applications since 2005, all 751 have been granted, as the following figure shows.

FIGURE 3: ORDERS FOR THE PRODUCTION OF TANGIBLE GOODS

Year	Number of applications to FISC under 50 U.S.C. § 1862(c)(2)	Number of applications granted by FISC
2005 ³³⁴	155	155
2006 ³³⁵	43	43
2007 ³³⁶	6	6
2008 ³³⁷	13	13

332. Letter from Peter J. Kadzik, Principal Deputy Assistant Attorney Gen., Office of Legislative Affairs, U.S. Department of Justice, to the Hon. Harry Reid, Majority Leader, U.S. Senate (Apr. 30, 2013), *available at* <https://www.fas.org/irp/agency/doj/fisa/2012rept.pdf>, [<http://perma.cc/0KymPaptHiZ>].

333. The government made a total of 1856 applications for electronic surveillance or physical searches; of those, 1789 included requests for electronic surveillance. Of those, one was withdrawn by the government prior to FISC ruling. *Id.*

334. Letter from William E. Moschella, Assistant Attorney Gen., Office of Legislative Affairs, U.S. Department of Justice, to the Hon. Richard B. Cheney, President, U.S. Senate (Apr. 28, 2006), *available at* http://www.justice.gov/nsd/foia/foia_library/2005fisa-ltr.pdf, [<http://perma.cc/UK7V-FQDN>].

335. Letter from Richard A. Hertling, Acting Assistant Attorney Gen., Office of Legislative Affairs, U.S. Department of Justice, to the Hon. Richard B. Cheney, President, U.S. Senate (Apr. 27, 2007), *available at* http://www.justice.gov/nsd/foia/foia_library/2006fisa-ltr.pdf, [<http://perma.cc/E9ME-5PEQ>].

336. Letter from Brian A. Benczkowski, Principal Deputy Assistant Attorney Gen., Office of Legislative Affairs, U.S. Department of Justice, to the Hon. Richard B. Cheney, President, U.S. Senate (Apr. 30, 2008), *available at* http://www.justice.gov/nsd/foia/foia_library/2007fisa-ltr.pdf, [<http://perma.cc/M5L7-3QGR>].

337. Letter from Ronald Weich, Assistant Attorney Gen., Office of Legislative Affairs, U.S. Department of Justice, to the Hon. Joseph R. Biden, Jr., President, U.S.

2009 ³³⁸	21	21
2010 ³³⁹	96	96
2011 ³⁴⁰	205	205
2012 ³⁴¹	212	212
Totals	751	751

It is important to underscore that the lack of more contextual data cautions against inferring too much from the nonexistent rate of denial. In passing the tangible goods provision, Congress tied the court's hands, *requiring* FISC to grant applications once the statutory conditions are met.³⁴² To the extent, then, that FISC is deferential to the executive, responsibility lies at least in part with the legislature. In addition, it is almost impossible to tell, outside of the classified world, the extent to which the court pushes back on the DOJ—not just in regard to specific orders, but in relation to broader rules and procedures, as well as in an oversight capacity. Two examples come to mind.

In 2010, John D. Bates, Presiding Judge of FISC, issued a declassified *Rules of Procedure*, requiring notice and briefing of nov-

Senate (May 14, 2009), *available at* http://www.justice.gov/nsd/foia/foia_library/2008fisa-ltr.pdf, [<http://perma.cc/RVY8-GWLR>].

338. Letter from Ronald Weich, Assistant Attorney Gen., Office of Legislative Affairs, U.S. Department of Justice, to the Hon. Joseph R. Biden, Jr., President, U.S. Senate (Apr. 30, 2010), *available at* http://www.justice.gov/nsd/foia/foia_library/2009fisa-ltr.pdf, [<http://perma.cc/MNA7-XGLD>].

339. Letter from Ronald Weich, Assistant Attorney Gen., Office of Legislative Affairs, U.S. Department of Justice, to the Hon. Joseph R. Biden, Jr., President, U.S. Senate (Apr. 29, 2011), *available at* http://www.justice.gov/nsd/foia/foia_library/2010fisa-ltr.pdf, [<http://perma.cc/3QQX-NK9W>].

340. Letter from Ronald Weich, Assistant Attorney Gen., Office of Legislative Affairs, U.S. Department of Justice, to the Hon. Joseph R. Biden, Jr., President, U.S. Senate (Apr. 30, 2012), *available at* http://www.justice.gov/nsd/foia/foia_library/2011fisa-ltr.pdf, [<http://perma.cc/57T5-CYR2>].

341. Letter from Peter J. Kadzik, Principal Deputy Assistant Attorney Gen., Office of Legislative Affairs, U.S. Department of Justice, to the Hon. Joseph R. Biden, Jr., President, U.S. Senate (Apr. 30, 2013), *available at* http://www.justice.gov/nsd/foia/foia_library/2012fisa-ltr.pdf, [<http://perma.cc/0tNcrgUS6nx>].

342. 50 U.S.C. § 1861(c)(1) (2006) (“Upon an application made pursuant to this section, if the judge finds that the application meets the requirements of subsections (a) and (b), the judge *shall* enter an ex parte order as requested, or as modified approving the release of tangible things.” (emphasis added)).

el issues before the court.³⁴³ This document suggested that FISC would not, in the future, simply accept applications in new areas of the law without first considering the underlying legal issues.

Second, the recently-released judicial opinions from 2009 suggest that FISC was pressuring the NSA with regard to its failure to ensure that the identifiers run against the database be subjected to a test of reasonable, articulable suspicion. The court was clearly uncomfortable with the pattern of misinformation that had marked the government's previous representations to FISC. But, these same documents also reveal the extent to which the court relies on the NSA to police its own activities—again raising questions about the extent to which FISC adequately performs its envisioned role. As a final note, it is important to recognize that the sheer volume of the numbers associated with the tangible goods provisions (751) is remarkable in part because any one order could result in the collection of millions of records on millions of people, as we have seen with the telephony metadata program. In light of the *in camera*, *ex parte* proceedings, these numbers raise further questions about FISC's role.

II. BULK COLLECTION AND FISA'S STATUTORY PROVISIONS

The telephony metadata program violates FISA's express statutory language in three areas: first, with regard to the language "relevant to an authorized investigation"; second, in relation to the requirement that the information sought be obtainable under subpoena *duces tecum*; and third, in its violation of the restrictions specifically placed on pen registers and trap and trace equipment.

A. "Relevant to an Authorized Investigation"

The government argues that the NSA's telephony metadata program is consistent with the language of 50 U.S.C. § 1861 in that *all* telephone calls in the United States, including those of a wholly

343. FISA CT. R. 11, available at <https://www.fas.org/irp/agency/doj/fisa/fiscrules-2010.pdf>, [<http://perma.cc/5K96-A4LZ>]. The current rules, issued November 1, 2010, superseded both the February 17, 2006 Rules of Procedure and the May 5, 2006 Procedures for Review of Petitions Filed Pursuant to Section 501(f) of the Foreign Intelligence Surveillance Act of 1978, As Amended.

local nature, are “relevant” to foreign intelligence investigations. The word “relevant” itself, the administration states, “is a broad term that connotes anything ‘[b]earing upon, connected with, [or] pertinent to a’ specified subject matter.”³⁴⁴ Turning to its “particularized legal meaning,” the government argues:

It is well-settled in the context of other forms of legal process for the production of documents that a document is ‘relevant’ to a particular subject matter not only where it directly bears on that subject matter, but also where it is reasonable to believe that it could lead to other information that directly bears on that subject matter.³⁴⁵

That massive amounts of data may be involved is of little import:

Courts have held in the analogous contexts of civil discovery and criminal and administrative investigations that ‘relevance’ is a broad standard that permits discovery of large volumes of data in circumstances where doing so is necessary to identify much smaller amounts of information within that data that directly bears on the matter being investigated.³⁴⁶

Applied to the telephony metadata program, though recognizing that the telephony metadata program is “broad in scope,” the government argues that there are nevertheless “reasonable grounds to believe” that the category of data (i.e., all telephone call data), when queried and analyzed, “will produce information pertinent to FBI investigations of international terrorism.”³⁴⁷ For communications data, the government argues, connections between individual data points can only be reliably identified through large-scale data mining.³⁴⁸ As DOJ explained to Congress: “The more metadata NSA has access to, the more likely it is that NSA can identify, discover and understand the network of contacts linked to targeted numbers or addresses.”³⁴⁹

344. SECTION 215 WHITE PAPER, *supra* note 2, at 9 (quoting 13 THE OXFORD ENGLISH DICTIONARY 561 (2d ed. 1989)).

345. *Id.*

346. *Id.* at 1–2.

347. *Id.* at 2.

348. *See id.*

349. DEP’T OF JUSTICE, REPORT ON THE NATIONAL SECURITY AGENCY’S BULK COLLECTION PROGRAMS FOR USA PATRIOT ACT REAUTHORIZATION 5 (2011), *available at* http://www.dni.gov/files/documents/2011_CoverLetters_Report_Collection.pdf, [<http://perma.cc/S7CD-E8Z7>].

There are two sets of responses to the government's arguments. The first centers on the government's claim that all telephony metadata is relevant. The second concerns the connection in the statutory language between the relevance of the information to be obtained and "an authorized investigation."³⁵⁰

1. *Relevance Standard*

Four legal arguments undermine the government's claim that there are "reasonable grounds" to believe that hundreds of millions of daily telephone records are "relevant" to an authorized investigation. First, the NSA's interpretation of "relevant" collapses the statutory distinction between relevant and irrelevant records, thus obviating the government's obligation to discriminate between the two. Second, this reading renders meaningless the qualifying phrases in the statute, such as "reasonable grounds." Third, the government's interpretation establishes a concerning legal precedent. Fourth, the broad reading of "relevant" contravenes congressional intent.

First, in ordinary usage, something is understood as relevant to another thing when a demonstrably close connection between the two objects can be established.³⁵¹ This is also the way in which courts have consistently applied the term to the collection of information—as with grand-jury subpoenas, where the information collected must bear some actual connection to a particular investigation.³⁵²

350. 50 U.S.C. § 1861(b)(2)(A)(i)–(iii) (2006).

351. *See, e.g.*, OXFORD AMERICAN DICTIONARY 1474 (3d ed. 2010) (defining relevant as "the state of being closely connected or appropriate to the matter in hand"); MERRIAM-WEBSTER'S COLLEGIATE DICTIONARY 1051 (11th ed. 2006) (defining "relevant" as "having significant and demonstrable bearing on the matter at hand"); *see also* Memorandum of Law in Support of Plaintiffs' Motion for a Preliminary Injunction at 9–12, *ACLU v. Clapper*, No. 13-cv-03994 (S.D.N.Y. Aug. 26, 2013), available at <https://www.aclu.org/files/pdfs/natsec/clapper/2013.08.26%20ACLU%20PI%20Brief.pdf>, [<http://perma.cc/CCV9-ZSHT>].

352. *See, e.g.*, *Cheney v. U.S. Dist. Court*, 542 U.S. 367, 383, 387–88 (2004) (noting that "overbroad" discovery orders were "anything but appropriate" because they "ask[ed] for everything under the sky"); *Bowman Dairy Co. v. United States*, 341 U.S. 214, 221 (1951) (overturning use of a "catch-all provision" in a subpoena on grounds that it was "merely a fishing expedition to see what may turn up"); *In re Horowitz*, 482 F.2d 72, 79 (2d Cir. 1973) (Friendly, J.) (narrowing a grand-jury subpoena because it improperly required an individual to turn over the contents

In contrast, almost none of the information the government obtained under the bulk metadata collection program is demonstrably linked to an authorized investigation. The government itself has admitted this. Writing to Representative James Sensenbrenner, Peter Kadzik, the Principal Deputy Assistant Attorney General, acknowledged, “most of the records in the dataset are not associated with terrorist activity.”³⁵³ FISC Judge Reggie Walton drew the point more strongly:

The government’s applications have all acknowledged that, of the [REDACTED] of call detail records NSA receives *per day* (currently over [REDACTED] per day), the vast majority of individual records that are being sought pertain neither to [REDACTED] . . . In other words, nearly all of the call detail records collected pertain to communications of non-U.S. persons who are *not* the subject of an FBI investigation to obtain foreign intelligence information, [and] are communications of U.S. persons who are *not* the subject of an FBI investigation to protect against international terrorism or clandestine intelligence activities.³⁵⁴

In other words, most of the information being collected does not relate to any individuals suspected of any wrongdoing.

In defense of its broad interpretation, the government argues that it must collect irrelevant information to ascertain what is relevant. This means that the NSA, in direct contravention of the statutory language, is collapsing the distinction between relevant and irrelevant records—a distinction that Congress required be made *before* collection. Because of this collapse, the NSA is gaining an extraordinary amount of information. The records the government sought under the telephony metadata program detail the daily interactions of millions of Americans who are not themselves connected in any way to foreign pow-

of multiple filing cabinets “without any attempt to define classes of potentially relevant documents or any limitations as to subject matter or time period”).

353. Letter from Peter J. Kadzik, Principal Deputy Assistant Attorney Gen., U.S. Department of Justice, to the Hon. F. James Sensenbrenner, Jr., U.S. House of Representatives 2 (July 16, 2013), *available at* <http://1.usa.gov/12GN8kW>, [<http://perma.cc/9F49-US7R>].

354. *In re* Production of Tangible Things from [REDACTED], BR 08-13, at 11–12 (FISA Ct. Mar. 2, 2009), *available at* http://www.dni.gov/files/documents/section/pub_March%202009%20Order%20from%20FISC.pdf, [<http://perma.cc/9YZ-CMCV>].

ers or agents thereof. They include private and public interactions between senators, between members of the House of Representatives, and between judges and their chambers, as well as information about state and local officials. They include parents communicating with their children's teachers, and zookeepers arranging for the care of animals. Metadata information from calls to rape hotlines, abortion clinics, and political party headquarters are likewise not exempt from collection—the NSA is collecting all telephony metadata.

Second, in addition to collapsing the distinction between relevant and irrelevant records, reading FISA to allow this type of collection would neuter the qualifying phrases contained in 50 U.S.C. § 1861(b)(2)(A). The statute requires, for instance, that there be “reasonable grounds” to believe that the records being sought are relevant.³⁵⁵ Although FISA does not define “reasonable grounds,” the Supreme Court has treated this phrase as the equivalent of “reasonable suspicion.”³⁵⁶ This standard requires a showing of “specific and articulable facts which, taken together with rational inferences from those facts, reasonably warrant” an intrusion on an individual’s right to privacy.³⁵⁷

The FISC order requires that Verizon disclose all domestic telephone records—including those of a purely local nature.³⁵⁸ According to Verizon Communications News Center, as of last year the company had 107.7 million wireless customers, connecting an average of 1 billion calls per day.³⁵⁹ It is impossible that the government provided specific and articulable facts showing reasonable grounds for the relevance of each one of those cus-

355. 50 U.S.C. § 1861(b)(2)(A).

356. *See, e.g.*, *United States v. Banks*, 540 U.S. 31, 36 (2003); *United States v. Hensley*, 469 U.S. 221, 227 (1985); *United States v. Brignoni-Ponce*, 422 U.S. 873, 881–82 (1975); KRIS & WILSON, *supra* note 167, § 19:3.

357. *Terry v. Ohio*, 392 U.S. 1, 21 (1968).

358. *In re Application of the FBI for an Order Requiring the Production of Tangible Things from Verizon Bus. Network Svcs.*, Secondary Order, BR 13-80, at 2 (FISA Ct. Apr. 25, 2013), available at <http://www.theguardian.com/world/interactive/2013/jun/06/verizon-telephone-data-court-order?guni=Article:in%20body%20link>, [<http://perma.cc/C6XM-RWNM>].

359. *Verizon Communications Company Statistics*, VERIZON COMMUNICATIONS NEWS CENTER, <http://www.statisticbrain.com/verizon-communications-company-statistics/>, [<http://perma.cc/J267-NK6Y>] (last visited March 13, 2014).

tomers or calls. Interpreting all records as relevant effectively renders the “reasonable grounds” requirement obsolete.

The statute does not explain precisely what makes a tangible item relevant to an authorized investigation. Nevertheless, the act suggests that tangible things are “presumptively relevant” when they:

[P]ertain to—(i) a foreign power or an agent of a foreign power; (ii) the activities of a suspected agent of a foreign power who is the subject of such authorized investigation; or (iii) an individual in contact with, or known to, a suspected agent of a foreign power who is the subject of such authorized investigation.³⁶⁰

This section appears not to apply to the telephony metadata program. It would be impossible to establish that all customer and subscriber records pertain to a foreign power or an agent thereof, or to a particular, suspected agent of the same, who is the subject of an authorized investigation. Perhaps five or ten customers may fall into this category, but to include millions simply pushes the bounds of common sense. Accordingly, the telephony metadata are neither relevant nor presumptively relevant.

Third, the breadth of the government’s interpretation establishes a troubling precedent. If all telephony metadata are relevant to foreign intelligence investigations, then so are all e-mail metadata, all GPS metadata, all financial information, all banking records, all social network participation, and all Internet use. Both the DOJ and FISC have suggested that there may be other programs in existence that operate in a similar fashion.³⁶¹ Some media reports appear to support this. On September 28, 2013, for instance, the *New York Times* reported that the NSA “began allowing the analysis of phone call and email logs in November 2010 to begin examining Americans’ networks of

360. 50 U.S.C. § 1861(b)(2)(A).

361. See, e.g., *In re Application of the FBI for an Order Requiring the Production of Tangible Things from [REDACTED]*, BR 13-109, at 19–20 (FISA Ct. Aug. 29, 2013), available at <http://www.uscourts.gov/uscourts/courts/fisc/br13-09-primary-order.pdf>, [<http://perma.cc/95LF-ACV7>] (“This Court has previously examined the issue of relevance for bulk collections. See [6 LINES OF REDACTED TEXT] While those matters involved different collections from the one at issue here, the relevance standard was similar.”).

associations.”³⁶² If all telephony metadata are relevant, then so are all other data—which means that very little would, in fact, be irrelevant to such investigations. If this is the case, then such an interpretation radically undermines not just the limiting language in the statute, but the very purpose for which Congress introduced FISA in the first place.

Fourth, the government’s interpretation directly contradicts Congress’s intent in adopting Section 215. At the introduction of the measure, Senator Arlen Specter explained that the language was meant to create an incentive for the government to use the authority only when it could demonstrate a connection to a *particular* suspected terrorist or spy.³⁶³ During a House Judiciary Committee meeting on July 17, 2013, Representative James Sensenbrenner (R-WI) reiterated that Congress inserted “relevant” into the statute to ensure that only information *directly related* to national security probes would be included—not to authorize the ongoing collection of all phone calls placed and received by millions of Americans not suspected of any wrongdoing.³⁶⁴ Soon afterwards, he wrote:

This expansive characterization of relevance makes a mockery of the legal standard. According to the administration, everything is relevant provided something is relevant. Congress intended the standard to mean what it says: The records requested must be reasonably believed to be associated with international terrorism or spying. To argue otherwise renders the standard meaningless.³⁶⁵

Other members of Congress have made similar claims.³⁶⁶

362. James Risen & Laura Poitras, *N.S.A. Examines Social Networks of U.S. Citizens*, N.Y. TIMES, Sep. 29, 2013, at A1.

363. 151 CONG. REC. 13,440 (2005).

364. *Oversight of the Administration’s Use of FISA Authorities: Hearing Before the H. Comm. on the Judiciary*, 113th Cong. (2013) (statement of Rep. James Sensenbrenner).

365. James Sensenbrenner, *How secrecy erodes democracy*, POLITICO, July 22, 2013, <http://politi.co/1baupnm>, [<http://perma.cc/9CG4-NM2Y>].

366. See, e.g., *Oversight of the Administration’s Use of FISA Authorities: Hearing Before the H. Comm. on the Judiciary*, 113th Cong. (July 17, 2013) (statement of Rep. Jerrold Nadler) (“[I]f we removed that word from the statute, [the government] wouldn’t consider . . . that it would affect [its] ability to collect meta-data in any way whatsoever, which is to say [it is] disregarding the statute entirely.”).

2. Connection to “an Authorized Investigation”

There are three ways in which the telephony metadata program violates FISA’s requirement in section 1861 that the order be sought for use in an “authorized investigation.”³⁶⁷ First, the guidelines establishing when such an investigation exists apply solely to the initial collection of the information. The FISC order, by contrast, allows the collection of the data on an ongoing basis, tying instead the *search* of such information to authorized investigations. Second, under the Attorney General guidelines, for each of the levels there is a predicate specificity required *before* the collection of information: namely, that the investigation be premised on specific individuals, groups, or organizations, or violations of criminal law. The telephony metadata program, in contrast, requires no such specificity *before* the collection of the data. Third, the orders issued by FISC empower the NSA to conduct searches of the data in *future* authorized investigations. In other words, the collection of the metadata is considered relevant to investigations generally. This means that the orders do not, in fact, relate to (existing) authorized investigations.

a. Collection of the Information

FISA, as mentioned above, requires that the government submit a statement of facts demonstrating reasonable grounds to believe that the records being sought are relevant to an authorized investigation (other than a threat assessment).³⁶⁸ Its definition of an “authorized investigation” refers to guidelines approved by the Attorney General under Executive Order 12,333.³⁶⁹ The most recent of these guidelines, the *Attorney General’s Guidelines for Domestic FBI Operations*, provides three categories of investigations: assessments (i.e., “threat assessments” under the 2003 guidelines and Section 215); predicated investigations (subdivided into “preliminary” and “full” investigations); and enterprise investigations (a variant of full investigations).³⁷⁰

367. 50 U.S.C. § 1861(b)(2)(A) (2006).

368. *Id.*

369. *Id.* § 1861(a)(2)(A).

370. U.S. DEP’T OF JUSTICE, THE ATTORNEY GENERAL’S GUIDELINES FOR DOMESTIC FBI OPERATIONS 16–18 (2008), available at <http://www.justice.gov/ag/readingroom/guidelines.pdf>, [<http://perma.cc/EU8-WC26>]; *Fact Sheet: Attorney General Consolidated guidelines for FBI Domestic Operations*, DEPARTMENT OF JUSTICE

FISA, as noted above, makes it clear that the tangible records in question may *not* be sought as part of the first level of national security investigations, the assessment stage.³⁷¹ There is an important reason for this restriction. It is the most general level and, as such, lacks the factual predicate required for the use of more intrusive techniques of information gathering.

Between 2003 and 2008, for instance, at the threat assessment stage the FBI could collect information on “individuals, groups, and organizations of possible investigative interest, and information on possible targets of international terrorist activities or other national security threats.”³⁷² But the only techniques allowed, as noted by the Attorney General, were “relatively non-intrusive investigative techniques.”³⁷³ This included:

(Oct. 3, 2008), available at <http://www.justice.gov/opa/pr/2008/October/08-ag-889.html>, [<http://perma.cc/MHT7-MSXY>] (noting that the new, consolidated guidelines “replace five existing sets of guidelines that separately addressed criminal investigations generally, national security investigations, and foreign intelligence collection, among other matters. In contrast to previous guidelines, the new guidelines are generally unclassified, providing the public with ready access in a single document to the basic body of operating rules for FBI activities within the United States”). For the previous guidelines, see U.S. DEP’T OF JUSTICE, THE ATTORNEY GENERAL’S GUIDELINES FOR FBI NATIONAL SECURITY INVESTIGATIONS AND FOREIGN INTELLIGENCE COLLECTION (2003), available at <http://www.fas.org/irp/agency/doj/fbi/nsiguilines.pdf>, [<http://perma.cc/7NPR-3SV3>] [hereinafter AG’S NSI GUIDELINES] (redacted in part); see also David S. Kris, *On the Bulk Collection of Tangible Things*, LAWFARE RES. PAPER SERIES, Sept. 29, 2013, at 17, available at <http://www.lawfareblog.com/wp-content/uploads/2013/09/Lawfare-Research-Paper-Series-No.-4-2.pdf>, [<http://perma.cc/3Z99-EJN9>]. Also note that on December 16, 2008, the FBI issued a Domestic Investigations and Operations Guide to help to implement the September 2008 Guidelines for Domestic FBI Operations. *FBI Records: the Vault*, FEDERAL BUREAU OF INVESTIGATION, available at <http://vault.fbi.gov/FBI%20Domestic%20Investigations%20and%20Operations%20Guide%20%28DIOG%29/fbi-domestic-investigations-and-operations-guide-diog-2008-version>, [<http://perma.cc/D29U-JPAW>]. A new FBI Domestic Investigations and Operations Guide was released Oct. 15, 2011 and updated June 15, 2012. See FED. BUREAU OF INVESTIGATION, DOMESTIC INVESTIGATIONS AND OPERATIONS GUIDE (2012), available at <http://www.aclu.org/files/pdfs/email-content-foia/FBI%20docs/June%202012%20FBI%20DIOG.pdf>, [perma.cc/ZPD5AVV3]. In addition to the AG-Dom (Attorney General’s Guidelines for Domestic FBI Operations), and the DIOG (Domestic Investigations and Operations Guide), every FBI HQ operational division has a PG (policy implementation guide) that supplements the DIOG. *Id.* at xxix.

371. 50 U.S.C. § 1861(b)(2)(A).

372. AG’S NSI GUIDELINES, *supra* note 370, at 3.

373. *Id.*

[O]btaining publicly available information, accessing information available within the FBI or Department of Justice, requesting information from other government entities, using online informational resources and services, interviewing previously established assets, non-pretexual interviews and requests for information from members of the public and private entities, and accepting information voluntarily provided by governmental or private entities.³⁷⁴

Nowhere in the discussion of the threat assessment stage did the 2003 guidelines contemplate the use of court-ordered surveillance.

In 2008, the Attorney General expanded the tools that could be used during the assessment stage to include: publicly available information; all available federal, state, local, tribal, or foreign governmental agencies' records; online services and resources; human source information; interviews or requests for information from members of the public and private entities; information voluntarily provided by governmental or private entities; observation or surveillance not requiring a court order; and grand jury subpoenas for telephone or electronic mail subscriber information.³⁷⁵ The addition of the last two items broadened the type of information that could be obtained. Similarly, whereas the previous guidelines noted that mail covers, mail openings, and nonconsensual electronic surveillance or any other investigative technique covered by 18 U.S.C. §§ 2510–2521 “shall not be used during a preliminary inquiry,”³⁷⁶ the 2008 guidelines dropped any equivalent language.

Even with the broadening, however, under FISA, tangible goods may not be obtained under section 215 during the assessment stage. The purpose is to place a higher burden on the government to justify the use of more intrusive surveillance. If such methods are to be used, and the related information collected,

374. *Id.*

375. U.S. DEP'T OF JUSTICE, ATTORNEY GENERAL'S GUIDELINES FOR DOMESTIC FBI OPERATIONS, *supra* note 370, at 20.

376. U.S. DEP'T OF JUSTICE, ATTORNEY GENERAL'S GUIDELINES ON GENERAL CRIMES, RACKETEERING ENTERPRISE AND DOMESTIC SECURITY/TERRORISM INVESTIGATIONS II(B)(5)(a)–(c) (1989), available at <http://www.justice.gov/ag/readingroom/generalcrimea.htm#general>, [<http://perma.cc/HP9Q-ZAXU>].

*there must be a factual predicate establishing a higher level of suspicion as to the presence of criminal activity or a threat to national security.*³⁷⁷

For preliminary investigations, this means that the government must have information or an allegation indicating the existence of criminal activity or a threat to U.S. national security prior to initiating the investigation.³⁷⁸ For a full investigation, there must be “an articulable factual basis for the investigation that reasonably indicates” criminal activity or a threat to U.S. national security.³⁷⁹ For an enterprise investigation (a variant of a full investigation), there must be an articulable factual basis for the investigation reasonably indicating “that the group or organization may have engaged or may be engaged in, or may have or may be engaged in planning or preparation or provision of support for” racketeering, international terrorism or other threats to U.S. national security, domestic terrorism, furthering political or social goals wholly or in part through activities that involve force or violence and a violation of federal criminal law, or a closed range of other offences.³⁸⁰ The guidelines thus distinguish between the different levels *based on a factual predicate of wrongdoing*, which then acts as a valve on the level of intrusiveness that the government can adopt in collecting more information.

In contrast, the primary order for the telephony metadata program does not follow this approach. Instead, it authorizes the collection of data for 90-day periods *without any factual predicate supporting the acquisition or collection of data*. It is thus incompatible with the approach adopted in the Attorney General’s guidelines. The order also shifts the emphasis to the analysis of such data—which is to be conducted in connection with an authorized investigation. This is not, however, what is required by the FBI’s own guidelines. It is the *collection* of such information that

377. The guidelines explain: “A predicated investigation relating to a federal crime or threat to the national security may be conducted as a preliminary investigation or a full investigation. A predicated investigation that is based solely on the authority to collect foreign intelligence may be conducted only as a full investigation.” U.S. DEP’T OF JUSTICE, ATTORNEY GENERAL’S GUIDELINES FOR DOMESTIC FBI OPERATIONS, *supra* note 370, at 21.

378. *Id.*

379. *Id.* at 21–22.

380. *Id.* at 23.

is premised on the existence of an authorized investigation—not the *subsequent analysis* of data in the course of the same.

b. Specificity

According to the Attorney General’s guidelines, for predicate investigations (for which tangible items orders under Section 215 may be sought) *specificity* is required before the collection of information—namely, the investigation must be premised on the past or present wrongdoing or foreign intelligence activities of specific individuals, groups, or organizations. The telephony metadata program, in contrast, collects all call records, without specifying the individuals, groups, or organizations of interest.

For the past decade, specificity has been integral to the guidelines’ approach. Under the 2003 Attorney General’s guidelines, for instance, preliminary investigations were authorized “when there is information or an allegation indicating that a threat to the national security may exist.”³⁸¹ Such investigations were particular, in that they related to specific individuals, groups, and organizations.³⁸²

Under the 2008 guidelines, a preliminary investigation must relate to “a” federal crime or threat to national security.³⁸³ For foreign intelligence gathering, the guidelines require that only full investigations be used.³⁸⁴ These are defined in singular terms, such as “[a]n activity constituting a federal crime or a threat to national security.”³⁸⁵ Alternatively, the circumstances may indicate that “[a]n individual, group, organization, entity is or may be a target of attack, victimization, acquisition, infiltration, or recruitment in connection with criminal activity.”³⁸⁶ For enterprise investigations, the text of the guidelines clearly refers to “the group or organization.”³⁸⁷

Not only are the investigations specific regarding the targets, they are specific regarding the facts that support the initiation of

381. AG’S NSI GUIDELINES, *supra* note 370, at 3.

382. *Id.* at 4.

383. U.S. DEP’T OF JUSTICE, ATTORNEY GENERAL’S GUIDELINES FOR DOMESTIC FBI OPERATIONS, *supra* note 370, at 21.

384. *Id.* at 22.

385. *Id.* at 21.

386. *Id.*

387. *Id.* at 23.

the predicate investigation. For enterprise investigations, this means that there must be “an articulable factual basis for the investigation that reasonably indicates that the group or organization” was involved in the commission of certain crimes and activities.³⁸⁸ Full investigations, in turn, require specific and articulable facts giving reason to believe that a threat to national security may exist.³⁸⁹ Like preliminary investigations, such inquiries are specific in that they may relate to individuals, groups, and organizations.³⁹⁰ In contravention of the Attorney General guidelines, the telephony metadata program collects data, using precisely those tools that are limited to preliminary and full investigations, absent the specificity otherwise required.

c. Future Authorized Investigations

Third, FISA contemplates the relevance of information to an investigation *already in existence* at the time the order is granted. The statutory language is very specific. Applications must include “a statement of facts showing that there are reasonable grounds to believe that the tangible things sought are relevant to an authorized investigation.”³⁹¹ The placement of the word “are” before the word “relevant” suggests that at the time the records are being sought, their relevance to an investigation must be established.

The orders issued by FISC, however, depart from the statutory language, empowering the NSA to obtain the data in light of their relevance to future “authorized investigations”—and requiring telecommunications companies to indefinitely provide such information in the future.³⁹² How can the court know that all such telephony data will be relevant to investigations that are not yet opened? As noted by amici in *In re Electronic Privacy In-*

388. *Id.*

389. *Id.* at 22.

390. *Id.* at 21.

391. 50 U.S.C. § 1861(b)(2)(A) (2006).

392. *In re* Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things from [REDACTED], No. BR 13-80, at 2–3 (FISA Ct. Apr. 25, 2013), available at http://www.dni.gov/files/documents/PrimaryOrder_Collection_215.pdf, [<http://perma.cc/TB5P-C8TZ>] (“[T]he court finds as follows: (1) There are reasonable grounds to believe that the tangible things sought are relevant to authorized investigations (other than threat assessments) being conducted by the FBI . . .”).

formation Center, Congress could have used any number of alternative auxiliary verbs—“such as ‘can’; ‘could’; ‘will’; or ‘might.’ But it chose not to do so. Instead, Congress required relevance to an investigation existing at the time of the application.”³⁹³

In addition, the information sought must be relevant “to an authorized investigation.” This is both singular (“an”) and past tense, in that it has already been “authorized.” The House Report that accompanied the first introduction of the business records provisions explained that the purpose of this language was to provide “for an application to the FISA court for an order directing the production of tangible items such as books, records, papers, documents and other items upon certification to the court that the records sought are *relevant to an ongoing foreign intelligence investigation*.”³⁹⁴ Yet, how can the court with any certainty suggest that all investigations in the future will be authorized?

The government’s argument, instead of centering on a particular investigation, appears to create a categorical exception for the collection of records. Specifically, it argues that when the government “has reason to believe that conducting a search of a broad collection of telephony metadata records will produce counterterrorism information . . . the standard of relevance under Section 215 is satisfied.”³⁹⁵ That is, the determination depends on the nature of the information to be extracted, not on the prior existence of a directly related, authorized investigation. “Authorized investigations” thus become merely a category for which the information is useful.³⁹⁶ The language in the FISC order is not “an authorized investigation,” but, rather, “authorized investigations.”³⁹⁷

That the government has one investigation open on al Qaeda, or even “thousands of open full or enterprise investigations on

393. Brief for Cato Institute as Amicus Curiae in support of Petitioner, *In re Electronic Privacy Information Center*, No. BR 13-58, at 4 (U.S. Aug. 12, 2013).

394. H.R. REP. NO. 107-236, pt. 1, at 61 (2001).

395. SECTION 215 WHITE PAPER, *supra* note 2, at 8–9.

396. *See id.* at 6 (“The telephony metadata records are sought for properly predicated FBI investigations into specific international terrorist organizations and suspected terrorists.”).

397. *See In re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things from [REDACTED]*, No. BR 13-80, at 2–3 (FISA Ct. Apr. 25, 2013), available at http://www.dni.gov/files/documents/PrimaryOrder_Collection_215.pdf, [<http://perma.cc/TB5P-C8TZ>].

terrorist groups or targets, and their sponsors, some or all of which could underlie the bulk telephony metadata collection applications and orders,”³⁹⁸ fails to justify the collection of so many records—indeed, most of those collected—that are not in any way directly connected to these authorized investigations. This interpretation, moreover, contradicts congressional intent. As Representative F. James Sensenbrenner, one of the principal authors of the USA PATRIOT Act, noted, “Congress intended to allow the intelligence communities to access targeted information for specific investigations. How can every call that every American makes or receives be relevant to a specific investigation? This is well beyond what the Patriot Act allows.”³⁹⁹

B. *Subpoena Duces Tecum*

The only express limit on the type of tangible item that can be subject to an order under 50 U.S.C. § 1861 is that it “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.”⁴⁰⁰ Although it may be said as a general matter that Congress intended intelligence collection to be subject to different standards than those that apply in a criminal context, in at least the provisions relevant to tangible goods, it is clear that a criminal standard governs the *type* of information that can be obtained via order. Specifically, the collection must be consistent with a subpoena duces tecum.

The government argues that the telephony metadata program is consistent with this provision, and that its determination must be given the highest level of deference by the courts.⁴⁰¹ FISC has expressed its agreement with the government’s position:

398. Kris, *supra* note 370, at 20.

399. Jim Sensenbrenner, *This abuse of the Patriot Act must end*, THE GUARDIAN, June 9, 2013, <http://www.theguardian.com/commentisfree/2013/jun/09/abuse-patriot-act-must-end>, [<http://perma.cc/UJW3-P4PG>].

400. 50 U.S.C. § 1861(c)(2)(D) (2006).

401. *See, e.g.*, Defendants’ Memorandum of Law in Opposition to Plaintiffs’ Motion for a Preliminary Injunction at 17 n.8, *ACLU v. Clapper*, 13-cv-3994 (S.D.N.Y. Oct. 1, 2013) (citing *United States v. R. Enters., Inc.*, 498 U.S. 292, 301 (1991) (grand jury subpoena challenged on relevancy grounds must be upheld unless “there is no reasonable possibility that the category of materials the Government seeks will

Call detail records satisfy [the subpoena duces tecum] requirement, since they may be obtained by (among other means) a ‘court order for disclosure’ under 18 U.S.C. § 2703(d). Section 2703(d) permits the government to obtain a court order for release of non-content records, or even in some cases of the contents of a communication, upon a demonstration of relevance to a *criminal* investigation.⁴⁰²

To evaluate the government’s claim, it is first necessary to consider the legal instrument. A subpoena duces tecum is a writ or process used to command a witness to bring with him and produce to the court books, papers, and other items, over which he has control and which help to elucidate the matter at hand.⁴⁰³ Unlike warrants, something less than probable cause is required.⁴⁰⁴ The rationale behind this is that the purpose of the instrument is not to conduct a search absent a suspect’s consent, but, rather, to obtain documents and information that the prosecution has concluded will be material in a case.⁴⁰⁵

The authority to issue a subpoena is not unlimited. Under the Federal Rules of Criminal Procedure, “the court may quash or modify the subpoena if compliance would be unreasonable or oppressive.”⁴⁰⁶ Precisely what counts as reasonable (or not) is heavily context-dependent.⁴⁰⁷ In *United States v. Nixon*,⁴⁰⁸ the Court laid out a three-part test, requiring the government to establish relevancy, admissibility, and specificity, in order to enforce a subpoena in the trial context.⁴⁰⁹

produce information relevant to the general subject of the grand jury’s investigation”), available at https://www.aclu.org/files/assets/2013.10.01_govt_oppn_to_pi_motion.pdf, [http://perma.cc/7BSL-PJ7T]; *NLRB v. Am. Med. Response, Inc.*, 438 F.3d 188, 193 (2d Cir. 2006) (in a proceeding to enforce an administrative subpoena, “the agency’s appraisal of relevancy” to its investigation “must be accepted so long as it is not obviously wrong,” and the “district court’s finding of relevancy” will be affirmed unless it is “clearly erroneous”).

402. *In re* Production of Tangible Things from [REDACTED], Supplemental Opinion, No. BR 08-13, at 2 n.1 (FISA Ct. Dec. 12, 2008).

403. 3 WILLIAM BLACKSTONE, COMMENTARIES *382.

404. *See* *United States v. R. Enters., Inc.*, 498 U.S. 292, 297 (1991).

405. Joshua Gruenspecht, “Reasonable” Grand Jury Subpoenas: Asking for Information in the Age of Big Data, 24 HARV. J.L. & TECH. 543, 544 (2011).

406. FED. R. CRIM. P. 17(c)(2).

407. *See* *New Jersey v. T.L.O.*, 469 U.S. 325, 337 (1985).

408. 418 U.S. 683 (1974).

409. *See id.* at 699–700.

The *Nixon* standard, however, does not apply in the context of grand jury proceedings.⁴¹⁰ In 1991 the Court explained:

The multifactor test announced in *Nixon* would invite procedural delays and detours while courts evaluate the relevancy and admissibility of documents sought by a particular subpoena Requiring the Government to explain in too much detail the particular reasons underlying a subpoena threatens to compromise the ‘indispensable secrecy of grand jury proceedings.’ Broad disclosure also affords the targets of investigation far more information about the grand jury’s workings than the Rules of Criminal Procedure appear to contemplate.⁴¹¹

The Court went on to note that this does not mean that the grand jury’s investigatory powers are limitless; to the contrary, they are still subject to Rule 17(c).⁴¹² Nevertheless, grand jury subpoenas are given the benefit of the doubt, with the burden of showing unreasonableness on the recipient seeking to avoid compliance.⁴¹³ For claims of irrelevancy, motions to quash “must be denied unless the district court determines that there is no reasonable possibility that the category of materials the Government seeks will produce information relevant to the general subject of the grand jury’s investigation.”⁴¹⁴

At the broadest level, then, the government’s assertion, at least with regard to the burden of proof regarding the information to be obtained and the deference afforded a grand jury subpoena, appears to be valid. But there are three critical flaws in the government’s reasoning: first, subpoenas may not be used for fishing expeditions; second, they must be focused on specific individuals or alleged crimes *prior to the collection of information*; and third, the emphasis is on past wrongdoing—not on potential future relationships and actions. In addition, remarkably, FISC has admitted that the telephony metadata order it issued violates the statutory language requiring that the information to be obtained comport with the requirements of a subpoena.

410. *R. Enters.*, 498 U.S. at 297–99.

411. *Id.* at 298–99 (citations and quotations omitted).

412. *Id.* at 299.

413. *Id.* at 301.

414. *Id.*

1. Fishing Expeditions

The government's contention, consistent with *United States v. R. Enterprises, Inc.*, is that to fall outside the statutory confines, there must be no reasonable possibility that the category of materials sought under Section 215 will produce relevant information.⁴¹⁵ Although that case did give a fair amount of latitude in the standard of relevancy applied to grand jury subpoenas, it also established important limits. "Grand juries," the Court wrote, "are not licensed to engage in arbitrary fishing expeditions."⁴¹⁶

In other words, subpoenas may not be used to obtain massive amounts of information from which evidence of wrongdoing—absent prior suspicion—can be derived. A grand jury, for example, could not convene in Bethesda, Maryland, and simply begin collecting telephony metadata, which it could subsequently mine to find evidence of criminal behavior. To the contrary, an investigator must have a reasonable suspicion that some document or communication exists, and that it is directly relevant to the investigation in question, for the Court to order its production.

The Court has used this logic to quash a subpoena duces tecum requiring that computer hard drives and floppy disks be produced.⁴¹⁷ The subpoena requested was held to be overbroad because the subpoenaed materials "contain[ed] some data concededly irrelevant to the grand jury inquiry."⁴¹⁸ Judge Mukasey quashed the subpoena on the grounds that the government could narrow the documents requested prior to acquisition.⁴¹⁹ He also rejected the claim that the broader sweep of information was justified by the breadth of the investigation underway: even an "expanded investigation" did "not justify a subpoena which encompassed documents completely irrelevant to its scope."⁴²⁰

415. See Defendants' Memorandum of Law in Opposition, *supra* note 401, at 18–19.

416. *R. Enters.*, 498 U.S. at 299.

417. *In re Grand Jury Subpoena Duces Tecum Dated November 15, 1993*, 846 F. Supp. 11, 12 (S.D.N.Y. 1994).

418. *Id.*

419. *Id.* at 13–14.

420. *Id.* (quotation marks omitted); see also *Hale v. Henkel*, 201 U.S. 43, 76–77 (1906) (finding a subpoena duces tecum "far too sweeping in its terms to be regarded as reasonable" where it did not "require the production of a single contract, or of contracts with a particular corporation, or a limited number of documents, but all understandings, contracts, or correspondence between" a company

As discussed above in relation to the relevance standard, almost all of the telephony metadata collected under Section 215 is unrelated to criminal activity. In Judge Reggie Walton's words, "Ordinarily, this alone would provide sufficient grounds for a FISC judge to deny the application."⁴²¹ The principle at work here was recognized by the Eastern District of New York: "While the standard of relevancy [as applied to subpoenas] is a liberal one, it is not so liberal as to allow a party 'to roam in shadow zones of relevancy and to explore matter which does not presently appear germane on the theory that it might conceivably become so.'"⁴²² A subpoena duces tecum may not be used to compel the production of records simply because at some point, in the future, they might become relevant.

In a world limited by the physical manifestation of evidence, practicality helped to cabin the scope of subpoenas. Technology may have changed what is possible in terms of the volume and nature of records that can be obtained and stored, and the level of insight that can be gleaned. But it does not invalidate the underlying principle. Subpoenas, even those issued by grand juries, may not be used to engage in fishing expeditions.

2. Specificity

Grand jury investigations are specific. That is, they represent investigations into particular individuals, or particular entities, in relation to which there is reasonable suspicion that some illegal behavior has occurred. The compelled production of records or items is thus limited by reference to the target of the investigation.

and six others, over a multi-year period); *Ealy v. Littlejohn*, 569 F.2d 219, 227 (5th Cir. 1978) ("When the grand jury goes on a fishing expedition in forbidden waters, the courts are not powerless to act."); *Cessante v. City of Pontiac*, No. CIV. A. 07-cv-15250, 2009 WL 973339, at *12 (E.D. Mich. Apr. 9, 2009) ("While some of the information sought may be relevant or lead to relevant information, the request for 'anything and everything' is overly broad and not narrowly tailored to meet the relevancy requirements of Fed. R. Civ. P. 26(b).").

421. *In re* Production of Tangible Things from [REDACTED], Order, No. BR 08-13, at 9 (FISA Ct. Mar. 2, 2009), available at http://www.dni.gov/files/documents/section/pub_March%20202009%20Order%20from%20FISC.pdf, [perma.cc/3YGG-NBTQ].

422. *In re* Fontaine, 402 F. Supp. 1219, 1221 (E.D.N.Y. 1975) (quoting *Broadway & Ninety Sixth St. Realty Co. v. Loew's, Inc.*, 21 F.R.D. 347, 352 (S.D.N.Y. 1958)).

If a grand jury were, for instance, focused on the potentially criminal acts of the head of a crime family in New York, absent reasonable suspicion of some sort of connection to the syndicate, it could not issue a subpoena for the telephone records of the Parent-Teacher's Association at Briarwood School in Santa Clara, California. In contrast, the Section 215 orders are broad and non-specific. That is, on the basis of no particular suspicion, all call records, many of which are of a purely local nature, are swept up by the NSA.⁴²³

In response to this argument, the government points out that there is some precedent in the law for the government to collect records in bulk that may be relevant to an investigation and then to subject such records to subsequent analysis to determine which items are, in fact, relevant. In one case, the Eighth Circuit upheld a subpoena, even though most of the records bore no relationship to any criminal activity.⁴²⁴ This case, however, fails to support the government's argument with regard to Section 215 and the bulk collection of metadata.

In *In re Grand Jury Proceedings*, the government served two grand jury subpoenas duces tecum on Western Union.⁴²⁵ The first required production of monthly wire transactions at the Royale Inn, Kansas City, Missouri, for a period of thirteen months.⁴²⁶ The second required production of Telegraphic Money Order Applications above \$1000 from the Royale Inn, Kansas City, Missouri, between January 1984 and February 1986.⁴²⁷ Western Union moved to quash the subpoenas on the ground that they amounted to an unreasonable search and seizure in violation of the Fourth Amendment.⁴²⁸ The government responded by alleging that drug dealers in Kansas City were using Western Union to transmit money.⁴²⁹

423. See *In re* an Application From the FBI for the Production of Tangible Things from [REDACTED], Order, No. 06-05, at 2 (FISA Ct. May 24, 2006), available at <http://s3.documentcloud.org/documents/785206/pub-may-24-2006-order-from-fisc.pdf>, [<http://perma.cc/FDS9-SYXE>].

424. *In re* Grand Jury Proceedings: Subpoena Duces Tecum, 827 F.2d 301 (8th Cir. 1987).

425. *Id.*

426. *Id.*

427. *Id.*

428. *Id.*

429. *Id.*

The Eighth Circuit noted that it had previously held that Western Union customers have no privacy interest in Western Union records.⁴³⁰ The court cited the Supreme Court's holding in *United States v. Miller*, in which the Supreme Court determined, consistent with *Smith v. Maryland*, that bank customers do not enjoy a legitimate expectation of privacy in bank records subject to subpoena.⁴³¹

The court in *In re Grand Jury* specifically noted that the request at issue—namely, the production of records from Royale Inn—was not as sweeping as subpoenas that the judiciary had found to be outside the bounds of acceptability. In *Federal Trade Commission v. American Tobacco Co.*, for instance, the Supreme Court refused to uphold the FTC's direction to two tobacco companies to produce letters and contracts.⁴³² The FTC had claimed "an unlimited right of access to the respondents' papers . . . relevant or irrelevant, in the hope that something [would] turn up."⁴³³ The Eighth Circuit similarly declined to uphold a subpoena calling for an attorney's records over a ten-year period.⁴³⁴ The collection of all U.S. persons' telephony metadata is more properly considered in the same league as *FTC v. American Tobacco Co.* and *Schwimmer v. United States*, in which the courts recognized the overbroad use of government authority, as opposed to the more limited collection of information at issue in *In re Grand Jury Proceedings*.

3. Past Crimes

Grand jury investigations are also retroactive, searching for evidence of a *past* crime. The telephony metadata orders, in contrast, are both past- and forward-looking, in that they anticipate the possibility of illegal behavior in the future. Although most of the individuals in the database are suspected of no wrongdoing whatsoever, the minimization procedures allow for any information obtained from mining the data to then be

430. *United States v. Gross*, 416 F.2d 1205, 1213 (8th Cir. 1969); accord *Newfield v. Ryan*, 91 F.2d 700, 703 (5th Cir. 1937).

431. *United States v. Miller*, 425 U.S. 435, 440–443 (1976).

432. See *FTC v. American Tobacco Co.*, 264 U.S. 298, 305 (1924).

433. *Oklahoma Press Publ'g Co. v. Walling*, 327 U.S. 186, 207 n.40 (quoting *FTC*, 264 U.S. at 305).

434. *Schwimmer v. United States*, 232 F.2d 855, 861–62 (8th Cir. 1956).

used in criminal prosecution. This is an unprecedented use of subpoena information-gathering authority amounting to a permanent, ongoing grand jury investigation into all possible future criminal acts.

4. March 2009 FISC Opinion

FISC has openly recognized that the information it obtains from the metadata program could not otherwise be collected with any other legal instrument—including a subpoena duces tecum. In a secret opinion in March 2009, Judge Reggie Walton wrote:

Because the collection would result in NSA collecting call detail records pertaining to [REDACTED] of telephone communications, including call detail records pertaining to communications of United States (U.S.) persons located within the U.S. who are not the subject of any FBI investigation and whose metadata *could not otherwise be legally captured in bulk*, the government proposed stringent minimization procedures that strictly controlled the acquisition, accessing, dissemination, and retention of these records by the NSA and FBI.⁴³⁵

Later in the document, he again noted that the information “otherwise could not be legally captured in bulk by the government.”⁴³⁶ These assertions directly contradict the statutory requirement that the information could otherwise be obtained via subpoena duces tecum and amount to an admission, by the court, that the program violated the statute.

What makes the the court’s failure to stop the illegal program even more concerning, perhaps, is Judge Walton’s explanation of why, even though the information could not legally be obtained in any other way, FISC allowed the government to proceed. He continued:

Nevertheless, the FISC has authorized the bulk collection of call detail records in this case based upon: (1) the government’s explanation, under oath, of how the collection of and access to such data are necessary to analytical methods that are vital to the national security of the United States; and (2)

435. *In re* Production of Tangible Things from [REDACTED], Order, BR 08-13, at 2 (FISA Ct. Mar.2, 2009), available at http://www.dni.gov/files/documents/section/pub_March%20202009%20Order%20from%20FISC.pdf, [perma.cc/X67-5REV].

436. *Id.* at 12.

minimization procedures that carefully restrict access to the BR metadata and include specific oversight requirements.⁴³⁷

In other words, FISC allowed an illegal program to operate because the government (1) promised that it was vital to U.S. national security, and (2) was directed by the court to police its own house by following the minimization procedures. The former is a flimsy excuse for allowing the executive branch to break the law. The latter highlights the extent to which the court, precisely because of the size of the collection program in question, was dependent on the NSA: "In light of the scale of this bulk collection program, the Court must rely heavily on the government to monitor this program to ensure that it continues to be justified . . . and that it is being implemented in a manner that protects the privacy interests of U.S. persons."⁴³⁸

Recall that Congress created FISC to protect U.S. persons' privacy interests. Congress did not anticipate that FISC would simply hand over this responsibility to the NSA.

C. *Evisceration of Pen-Trap Provisions*

All of the information obtained through the telephony metadata program is already provided for in FISA's pen register and trap and trace provisions.⁴³⁹ The FISC order requires that telecommunication service providers turn over all telephony metadata between the United States and abroad or wholly with-

437. *Id.*

438. *Id.*

439. The government recently declassified two FISC opinions about a bulk electronic communications metadata program conducted under the Pen Register and Trap and Trace provisions of FISA. The program reportedly was ended because it failed to deliver the operational value expected. Although acknowledging the operational similarities, no discussion has been made public as to why the telephony metadata program was not conducted under section 402 of FISA, as its electronic communications bulk metadata collection counterpart was. See Press Release, Office of the Dir. of Intelligence, DNI Clapper Declassifies Additional Intelligence Community Documents Regarding Collection Under Section 501 of the Foreign Intelligence Surveillance Act (Nov. 18, 2013), available at <http://www.dni.gov/index.php/newsroom/press-releases/191-press-releases-2013/964-dni-clapper-declassifies-additional-intelligence-community-documents-regarding-collection-under-section-501-of-the-foreign-intelligence-surveillance-act-nov>, [perma.cc/54VA-5H6A].

in the United States, including local telephone calls.⁴⁴⁰ Telephony metadata, in turn, includes “comprehensive communications routing information, including but not limited to session identifying information (e.g., originating and terminating telephone number, International Mobile Subscriber Identity (IMSI) number, International Mobile station Equipment Identity (IMEI) number, etc.), trunk identifier, telephone calling card numbers, and time and duration of call.”⁴⁴¹ It does not include the name, address, or financial information of a subscriber or customer.⁴⁴²

Under FISA subchapter three, the government may obtain customers’ and subscribers’ telephone numbers, local or long distance telephone records, and “any records reflecting the period of usage (or sessions) by the customer or subscriber.”⁴⁴³ The government may also obtain any “associated routing or transmission information” related to the telephone or instrument number of the customer or subscriber.⁴⁴⁴

Unlike the NSA’s current practice, however, *each order* under the pen-trap provisions must be approved by either FISC or a magistrate judge appointed for the purpose of approving pen-trap orders under FISA.⁴⁴⁵ Orders must specify the precise identity (if known) of the person who is the subject of the investigation, and the person to whom is leased or in whose name the telephone line is listed.⁴⁴⁶ Heightened protections are provided for U.S. persons: collection may not be conducted solely on the basis of otherwise protected First Amendment activity.⁴⁴⁷

440. *In re* Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things from Verizon Business Network Services, Inc., No. BR 13-80, at 2 (FISA Ct. July 19, 2013), available at <http://www.theguardian.com/world/interactive/2013/jun/06/verizon-telephone-data-court-order?guni=Article:in%20body%20link>, [perma.cc/V53B-RM2D].

441. *Id.*

442. *Id.*

443. 50 U.S.C. § 1842d (2006).

444. *Id.*

445. *Id.* § 1842(b)(2).

446. *Id.* § 1842(d)(2)(A)(i)-(ii).

447. *Id.* § 1842(c)(2) (requiring “certification by the applicant 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”).

What the NSA is doing with the telephony metadata program is essentially obtaining all of this same information, without first making a particularized showing in relation to the target, obtaining an individualized court order, or ensuring the U.S. persons' data are given heightened protection. The issue is thus not whether U.S. persons' data are being collected "solely on the basis of otherwise protected First Amendment activity" —but that they are being collected *without any individualized suspicion and on no basis whatsoever*. In essence, the NSA has sidestepped the carefully-constructed protections of subchapter three to collect all telephony metadata.

D. Potential Violation of Other Provisions of Criminal Law

There are, in addition, other statutory provisions that raise questions about the legality of the current telephony metadata program. In December 2008, FISC issued a "Supplemental Opinion" giving the court's reasons for concluding that the records to be produced pursuant to the telephony metadata orders were properly subject to production under 50 U.S.C. § 1861.⁴⁴⁸ The reason behind the order appears to be that, although such orders were previously approved, for the first time the government had identified the provisions of 18 U.S.C. §§ 2702–2703 that are relevant to the question.

Under 50 U.S.C. § 1861, Congress empowered the government to apply to FISC "for an order requiring the production of *any* tangible things (including books, records, papers, documents, and other items)."⁴⁴⁹ The court placed special emphasis on the use of the word "any," suggesting that it "naturally connotes 'an expansive meaning,' extending to all members of a common set, unless Congress employed 'language limiting [its] breadth.'"⁴⁵⁰

448. *In re* Production of Tangible Things From [REDACTED], Supplemental Opinion, No. BR 08-13, at 1 (FISA Ct. Dec. 12, 2008), available at http://www.dni.gov/files/documents/section/pub_Dec%2012%202008%20Supplemental%20Opinions%20from%20the%20FISC.pdf, [http://perma.cc/X2ZR-9TM2].

449. 50 U.S.C. § 1861(a)(1) (emphasis added).

450. *In re* Production of Tangible Things From [REDACTED], Supplemental Opinion, No. BR 08-13, at 1 (FISA Ct. Dec. 12, 2008), available at http://www.dni.gov/files/documents/section/pub_Dec%2012%202008%20Supplemental%20Opinions%20from%20the%20FISC.pdf, [http://perma.cc/X2ZR-9TM2] (quoting *United States v. Gonzales*, 520 U.S. 1, 5 (1997)).

The court had apparently considered “any” to be without limit, until 18 U.S.C. §§ 2702–2703 was brought to its attention.⁴⁵¹ This statute laid out an apparently exhaustive set of circumstances under which telephone service providers could provide customer or subscriber records to the government.⁴⁵² An order under 50 U.S.C. § 1861 was not included in this list.⁴⁵³ At the same time that Congress had passed section 215 of the USA PATRIOT Act, moreover, it had amended sections 2702 and 2703 in ways that appeared to re-affirm that communications service providers could only divulge records to the government in particular circumstances—without specifically noting FISC orders.⁴⁵⁴

Judge Walton reconciled this tension in a most curious manner. He pointed to National Security Letters—a completely different form of subpoena (i.e., an administrative subpoena), noting that in the USA PATRIOT Act, Congress empowered the FBI, without prior judicial review, to compel a telephone service provider to produce “subscriber information and toll billing records information,” on the basis of FBI certification of relevance to an authorized foreign intelligence investigation.⁴⁵⁵ Judge Walton pointed to the heightened requirements of Section 1861, i.e., that the government provide a “statement of facts showing that there are reasonable grounds to believe that the tangible things sought are relevant” to a foreign intelligence investigation, and that FISC determine that the application is sufficient.⁴⁵⁶ He then noted that Section 2703(c)(2) expressly permits the government to use administrative

451. *Id.* at 3.

452. 18 U.S.C. § 2702(a)(3) (establishing that, except as provided in § 2702(c), a provider “shall not knowingly divulge a record or other [non-content] information pertaining to a subscriber or customer . . . to any governmental entity”); *id.* § 2703(c)(1) (“A governmental entity may require a provider . . . to disclose a record or other [non-content] information pertaining to a subscriber . . . or customer . . . only when the governmental entity” proceeds according to one of the potential routes laid out in § 2703(c)(1)(A)–(E) (2013).).

453. 18 U.S.C. § 2703(c)(1).

454. *In re* Production of Tangible Things From [REDACTED], Supplemental Opinion, No. BR 08-13, at 3 (FISA Ct. Dec. 12, 2008), *available at* http://www.dni.gov/files/documents/section/pub_Dec%2012%202008%20Supplemental%20Opinions%20from%20the%20FISC.pdf, [<http://perma.cc/X2ZR-9TM2>].

455. *Id.*; 18 U.S.C. § 2709(a).

456. 50 U.S.C. § 1861(b)(2)(A).

subpoenas to obtain certain categories of non-content information from a provider—and concluded that Congress surely could not have intended a higher standard for FISC orders.⁴⁵⁷

The problem with his reasoning is that despite the precision of 18 U.S.C. §§ 2702–2703 and the concurrent amendment of these sections with the introduction of USA PATRIOT Act section 215, Congress nowhere included in the language of 18 U.S.C. §§ 2703–2703 provision for FISC orders as an exception to the closed set. Instead, it allowed the provision of telephony metadata to the government only in two cases: first, when the governmental entity uses an administrative subpoena authorized by a federal or state statute; or, second, when a federal or state grand jury or trial subpoena issues.⁴⁵⁸ The next paragraph, moreover, ties the provision directly to the actual commission of a crime. A court order for disclosure under Section 2703(c) may only be issued by a court of competent jurisdiction where the government can provide “specific and articulable facts showing that there are reasonable grounds to believe that . . . the records or other information sought, are relevant and material to an ongoing criminal investigation.”⁴⁵⁹ The types of records the FBI sought from FISC, by contrast, extended well beyond records either relevant or material to an ongoing criminal investigation. Furthermore, under 18 U.S.C. § 2703(d), the judiciary is empowered to quash or modify such orders where the records being requested “are unusually voluminous in nature.”⁴⁶⁰ It would be difficult to imagine any telephony metadata database more voluminous than one collecting *all* call data in the United States. As such, the statute contemplates yet further limits on the collection of information.

457. 18 U.S.C. § 2703(c)(2); *In re* Production of Tangible Things From [REDACTED], Supplemental Opinion, No. BR 08-13, at 3 (FISA Ct. Dec. 12, 2008), available at http://www.dni.gov/files/documents/section/pub_Dec%2012%202008%20Supplemental%20Opinions%20from%20the%20FISC.pdf, [<http://perma.cc/X2ZR-9TM2>].

458. *Id.* § 2703(b)(1)(B).

459. *Id.* § 2703(d).

460. *Id.*

III. CONSTITUTIONAL CONSIDERATIONS

In its White Paper, the government argues that the telephony metadata collection program complies with the Constitution.⁴⁶¹ In so doing, it relies on *Smith v. Maryland*, in which the Supreme Court held that participants in telephone calls lack a reasonable expectation of privacy (for purposes of the Fourth Amendment) in the telephone numbers dialed and received on one's phone.⁴⁶² Judge Eagan similarly relies on *Smith* in her August 2013 memorandum opinion on the bulk collection program.⁴⁶³ It is the *only* Supreme Court Fourth Amendment case that she directly discusses, on the grounds that it is dispositive of the question of whether the NSA has the authority to collect all telephony metadata.⁴⁶⁴

The government's reliance on *Smith v. Maryland* is problematic. The case involved individualized, reasonable cause to believe that the target of the pen register engaged in criminal behavior and threatening and obscene conduct.⁴⁶⁵ The placement of the pen register, moreover, was obtained via consent.⁴⁶⁶ Most importantly, significant technological and societal changes mean that the intrusiveness of the technology and the resultant harm to U.S. citizens' privacy interests are fundamentally different from the situation that the Court confronted in 1979.

The cornerstone of the government's argument is *Katz v. United States*, a case in which the Supreme Court supplemented trespass doctrine with a reasonable expectation of privacy.⁴⁶⁷ But *Katz* itself was an effort by the Court to understand the Fourth Amendment in light of changing technologies. Since that time, tension has developed into what is now a split on the Court between those who consider Fourth Amendment incursions in terms of physical trespass, and those who adopt the reasoning of

461. See SECTION 215 WHITE PAPER, *supra* note 2, at 19.

462. *Smith v. Maryland*, 442 U.S. 735, 745 (1979).

463. *In re* Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things from [REDACTED], No. BR 13-109, at 6 (FISA Ct. Aug. 29, 2013).

464. *Id.*

465. *Smith*, 442 U.S. at 737.

466. *Id.*

467. *Katz v. United States*, 389 U.S. 347, 359 (1967).

Katz more broadly. Thus, a series of cases involving thermal scanners,⁴⁶⁸ GPS devices,⁴⁶⁹ and highly-trained dogs⁴⁷⁰ have divided along these lines.

Regardless of which approach one adopts, there is a strong argument that bulk collection falls within constitutional protections. The telephony metadata program amounts to a general warrant, the prohibition of which gave rise to the Fourth Amendment. The reason such warrants were rejected is because they amounted to granting the government an indefinite right of trespass, for which redress (because of their execution with legal sanction) could not be sought. Beyond the general warrant concern, the bulk telephony metadata program digitally trespasses on the private lives of U.S. citizens.

Under the reasonable expectation of privacy test, Americans do not expect that information provided to telephone service providers will be collected wholesale by the government to ascertain whom they call, who calls them, how long they talk, and where they are located when they do so. Most Americans do not even realize that they are providing this information to their telephone companies when they make a phone call. Nor do they realize the significant social network and substantive analysis that can be performed on this data to generate new insights into their private lives.

A variant of the government's argument suggests that the only point at which an individual has a privacy interest is not at the moment of acquisition of data, but at the moment when the data is subjected to individual queries or logarithmic processing. That is, the "search" in question relies on two additional considerations: (a) whether knowledge is being extracted (or further knowledge is being generated) from a broader data set comprised of third party data and (b) whether a human interlocutor is involved in the exchange.

There are a number of problems with this approach. In addition to the trespass and reasonable expectation considerations discussed above, the Supreme Court has never carved out an "automation exception" to the Fourth Amendment. It is at the

468. See, e.g., *Kyllo v. United States*, 533 U.S. 27 (2001).

469. See, e.g., *United States v. Jones*, 132 S. Ct. 945 (2012).

470. See, e.g., *Florida v. Jardines*, 133 S. Ct. 1409 (2013).

point that the thermal imaging device records heat signatures, that the GPS chip is attached, and that the dog steps onto the porch, that the search has occurred. That is the point at which an individual's private information is recorded. In addition, human beings have been involved in the process all the way along—regardless of the nature of the collection device. A human being makes the decision to obtain telephony metadata and to record it. Human beings program the equipment and arrange for it to be activated and to receive the information. They decide how it will be stored, accessed, and shared in the future. Analysis of the data is simply the final step in a long series of human decisions.

A final argument offered in support of the program is that, even if privacy interests are recognized, the national security interests at stake override whatever privacy intrusion arises from the bulk collection of telephony metadata.⁴⁷¹ Variants of this argument emphasize threats that the country faces and the extent to which access to information significantly strengthens the intelligence community's hand. DOJ explained to Congress: "[T]hese . . . collection programs significantly strengthen the Intelligence Community's early warning system for the detection of terrorists and discovery of plots against the homeland."⁴⁷² This claim lacks specificity. Usefulness qua usefulness is never sufficient justification for overriding statutory or constitutional constraints.

A. *The Problem with Smith v. Maryland*

The Fourth Amendment establishes "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures."⁴⁷³ In 1967, the Supreme Court interpreted this language in a manner that protected people, not places.⁴⁷⁴ Justice Stewart, writing for the Court, explained, "What a person knowingly exposes to the

471. U.S. DEP'T OF JUSTICE, Report on the National Security Agency's Bulk Collection Programs for USA PATRIOT Act Reauthorization 5 (2011), available at http://www.dni.gov/files/documents/2011_CoverLetters_Report_Collection.pdf, [<http://perma.cc/J6WA-4C6V>].

472. *Id.*

473. U.S. CONST. amend. IV.

474. *Katz v. United States*, 389 U.S. 347, 351 (1967).

public, even in his own home or office, is not a subject of Fourth Amendment protection. But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected."⁴⁷⁵ As Justice Harlan noted in his concurrence, the question is both subjective and objective: An individual must have exhibited an actual expectation of privacy and that expectation must "be one that society is prepared to recognize as 'reasonable.'"⁴⁷⁶ Resultantly, "a man's home is, for most purposes, a place where he expects privacy, but objects, activities, or statements that he exposes to the 'plain view' of outsiders are not 'protected' because no intention to keep them to himself has been exhibited."⁴⁷⁷

In *Smith v. Maryland*, the Supreme Court held that a pen register placed on a telephone line did not constitute a search within the meaning of the Fourth Amendment, because persons making phone calls do not have a reasonable expectation that the numbers they dial will remain private.⁴⁷⁸ The key sentence from the decision centered on the customer's relationship with the telephone company: "A person has no legitimate expectation of privacy in information he voluntarily turns over to third parties."⁴⁷⁹ It is this sentence that spawned what has come to be known as the "third party doctrine."⁴⁸⁰

The government relies on this opinion and the resultant third-party doctrine to argue that the telephony metadata program is constitutional. In the DOJ's August 2013 White Paper, it suggests that a Section 215 order is not a search because "the Supreme Court has expressly held participants in telephone calls lack any reasonable expectation of privacy under the Fourth Amendment in the telephone numbers dialed."⁴⁸¹ In *ACLU v. Clapper*, the government again cited to the Court's rea-

475. *Id.* at 351–52 (citations omitted).

476. *Katz*, 389 U.S. at 361 (Harlan, J., concurring).

477. *Id.*

478. *Smith v. Maryland*, 442 U.S. 735, 743–46 (1979).

479. *Id.* at 743–44.

480. *See also* *United States v. Miller*, 425 U.S. 435, 443 (1976) (extending the third party doctrine to banking records). *But see* *United States v. Warshak*, 631 F.3d 266, 288 (6th Cir. 2010) (declining to extend the third party doctrine to an e-mail stored with an Internet Service Provider on the grounds that customers have a reasonable expectation of privacy in their e-mail).

481. SECTION 215 WHITE PAPER, *supra* note 2, at 19.

soning in *Smith v. Maryland* that, even if a subscriber harbored a subjective expectation that the numbers dialed would remain private, it would not be reasonable because individuals have “no legitimate expectation of privacy in information” voluntarily turned over “to third parties.”⁴⁸² The government suggested that because courts subsequently followed *Smith* to find no reasonable expectation of privacy in the sending or receipt of e-mail and Internet protocol addressing information, as well as subscriber information, “*Smith* is fatal to Plaintiffs’ claim that the collection of metadata records of their communications violates the Fourth Amendment.”⁴⁸³

Judge Eagan similarly relied almost exclusively on *Smith v. Maryland* in her August 2013 opinion: “The production of telephone service provider metadata is squarely controlled by the U.S. Supreme Court decision in *Smith v. Maryland*.”⁴⁸⁴ She reasoned that because customers are aware that telephone service providers maintain call detail records in the normal course of business, customers assume the risk that the telephone company will provide those records to the government.⁴⁸⁵ That information was collected in bulk was of no consequence: “[W]here one individual does not have a Fourth Amendment interest, grouping together a large number of similarly-situated individuals cannot result in a Fourth Amendment interest springing into existence *ex nihilo*.”⁴⁸⁶

The problem with these arguments is that they fail to consider the specific facts and circumstances in *Smith*. They also fail to address critical ways in which the privacy interests impacted by

482. Defendants’ Memorandum of Law in Support of Motion to Dismiss the Complaint at 32–33, *ACLU v. Clapper*, No. 13-cv-03994 (S.D.N.Y. Aug. 26, 2013) (quoting *Smith*, 442 U.S. at 743–744).

483. *Id.* at 33.

484. *In re* Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things from [REDACTED], No. BR 13-109 slip op. at 6. The only other case directly cited in Judge Eagan’s Fourth Amendment discussion appears to be a decision of the FISA court itself, with secondary citations. The details of the secret court opinion that she cites as precedent, however, are redacted. *Id.* at 8.

485. *Id.* at 7–8.

486. *Id.* at 9.

the use of pen registers and their application to broad sectors of the population have changed as technology has advanced.⁴⁸⁷

First, consider the facts of *Smith v. Maryland*. On March 5, 1976, Patricia McDonough was robbed in Baltimore, Maryland.⁴⁸⁸ After giving the police a description of the robber and a 1975 Monte Carlo she had seen near the scene of the crime, she started receiving threatening and obscene phone calls from a man who identified himself as the robber.⁴⁸⁹ At one point, the caller asked her to go out in front of her house.⁴⁹⁰ When she did, Ms. McDonough saw the 1975 Monte Carlo moving slowly past her home.⁴⁹¹ On March 16, the police observed a car of the same description in her neighborhood.⁴⁹² Tracing the license plate, police discovered that the car was registered to Michael Lee Smith.⁴⁹³

The following day, the police asked the telephone company, without a warrant, to install a pen register to trace the numbers called from Smith's home telephone.⁴⁹⁴ The company agreed, and that same day Smith called Ms. McDonough's home.⁴⁹⁵ On the basis of this and other information, the police applied for and obtained a warrant to search Smith's house.⁴⁹⁶ Upon executing the warrant, police found a telephone book with the corner turned down to Ms. McDonough's name and number.⁴⁹⁷ In a subsequent six-man lineup, Ms. McDonough identified Smith as the person who robbed her.⁴⁹⁸

Although the police did not obtain a warrant prior to installing the pen register, at a minimum, reasonable suspicion had been established that the target of the surveillance, Michael Lee Smith, had robbed, threatened, intimidated, and harassed Patricia McDonough. The police, accordingly, installed the pen

487. This failure further underscores the absence of opposing counsel—an omission that would seem to be of particular import when assessing constitutional concerns.

488. *Smith v. Maryland*, 442 U.S. 735, 737 (1979).

489. *Id.*

490. *Id.*

491. *Id.*

492. *Id.*

493. *Id.*

494. *Id.*

495. *Id.*

496. *Id.*

497. *Id.*

498. *Id.*

register consistent with their reasonable suspicion that Smith was engaged in criminal wrongdoing.

The telephony metadata program is an entirely different situation. The NSA is engaging in bulk collection absent any reasonable suspicion that the individuals, whose telephone information is being collected, are engaged in *any* wrongdoing. To the contrary, almost all of the information obtained will bear no relationship whatsoever to criminal activity. The government, however, wants to place a pen register and trap and trace on all U.S. persons—essentially treating everyone in the United States as though they are Michael Lee Smith.

In *Smith*, the police wanted only to record the numbers dialed from the suspect's telephone.⁴⁹⁹ Although it is now often forgotten, at the time the case was decided telephone companies were treated as utilities, with local telephone calls billed by the minute. What was unique about the technology involved in the pen register was that it could both identify and record the numbers dialed from a telephone—a function that the phone company itself did not have. The purpose of the pen register was therefore specific and limited.

By contrast, the bulk collection program now collects the numbers dialed, the numbers that call a particular number, trunk information, and session times. While the police in 1976 were concerned with whether Michael Lee Smith was calling one specific number, the NSA metadata program now collects all numbers called—in the process obtaining significant amounts of information about individuals. Calls to a rape crisis line, an abortion clinic, a suicide hotline, or a political party headquarters reveal significantly more information than what was being sought in *Smith*. This makes the sheer amount of information available significantly different.

Trunk information, moreover, reveals not just the target of a particular telephone call, but where the callers and receivers are located.⁵⁰⁰ At the time of *Smith*, the police were only able to tell when someone was located at Smith's home. The telephone

499. *Id.* at 737.

500. *Hearing on Continued Oversight of the Foreign Intelligence Surveillance Act Before the S. Comm. on the Judiciary*, 113th Cong. 3 (2013) (written testimony of Edward W. Felten, Professor, Princeton Univ.).

did not follow Smith around. In contrast, mobile technologies now allow the police to ascertain where persons are located, creating a second layer of surveillance based simply on trunk identifier information. The bulk collection of records, moreover, means that the government has the ability to do that for not just one person, but for the entire country.

Further characteristics distinguish the case. In *Smith v. Maryland*, for instance, the police sought the information for a short period. The bulk metadata collection program, by contrast, while continued at 90-day intervals, has been operating for seven years now and the NSA argues that it should be a permanent part of the government surveillance program.

In *Smith*, the telephone company consented to placing the pen register on the line. There was no element of compulsion involved. This is a critical element in the analysis. The Fourth Amendment only applies to government actors. To the extent, then, that private companies are acting in their private capacities, the Fourth Amendment does not apply. In 1989, however, the Supreme Court considered a case in which a railroad company conducted drug testing on employees at the behest of the government.⁵⁰¹ The Supreme Court held that when private actors act under compulsion of the sovereign authority, they must be viewed as an instrument or agent of the government.⁵⁰²

In the case of the telephony metadata program (and in contrast to the situation in *Smith v. Maryland*), the government is compelling the telephone companies to produce all telephony metadata, under court order and with threat of sanction for failing to abide by the terms of the secondary order. The telecommunication service providers are thus acting directly at the behest of the government and, as such, should be considered within the reach of the Fourth Amendment.

Perhaps the most important difference between the two situations lies in the realms of technology and social construction. The extent to which we rely on electronic communications to conduct our daily lives is of a fundamentally different scale and complexity than the situation that existed at the time the Court heard arguments in *Smith*. Resultantly, the extent of in-

501. *Skinner v. Ry. Labor Execs.' Ass'n*, 489 U.S. 602 (1989).

502. *Id.* at 614.

formation that can be learned about not just individuals, but about neighborhoods, school boards, political parties, Girl Scout troops—indeed, about any social, political, or economic network—simply by the placement of a pen register or trap and trace, is far beyond what the Court contemplated in 1979.

B. More Intrusive Technologies and Their Impact on Privacy

The government argues that even if one sets aside *Smith v. Maryland* and considers the collection of telephony metadata to be a search, it is nevertheless reasonable.⁵⁰³ This claim dramatically understates both the evolution of technology and the intrusiveness of the program. Millions of Americans' communications are currently being tracked. The data include intimate details about U.S. citizens' lives that can be mined for further information. Significant social analysis can also be conducted on the data. Sophisticated algorithms, for instance, can be applied to pen register information to ascertain where the important nodes are in a network. Alliances, friendships, and predilections can be uncovered by studying patterns in behavior. And unlike raw content, the type of information that can be gleaned is ordered—making it in some ways even more useful than content itself.

Consider the sheer volume of communications being monitored. Although the FISC orders that the government has released and acknowledged relate solely to one company (Verizon), officials have also acknowledged that the acquisition of telephony metadata extends to the largest telephone service providers in the United States: Verizon, AT&T, and Sprint.⁵⁰⁴ This means that every time the average U.S. citizen makes a telephone call, the NSA is collecting the location, the number called, the time of the call, and the length of the conversation.⁵⁰⁵ The numbers are worth noting. According to the *Wall Street*

503. Defendants' Memorandum of Law in Opposition to Plaintiffs' Motion for a Preliminary Injunction at 25, *ACLU v. Clapper*, No. 13-cv-3994 (S.D.N.Y. Aug. 26, 2013), available at https://www.aclu.org/files/assets/2013.10.01_govt_oppn_to_pi_motion.pdf, [<http://perma.cc/4LLN-4L56>] (arguing that “[a]ny intrusion on privacy is minimal . . . because only telephony metadata are collected”).

504. Siobhan Gorman et al., *U.S. Collects Vast Data Trove*, *WALL ST. J.*, June 7, 2013, <http://on.wsj.com/11uDoue>, [<http://perma.cc/0DAai1LuBvy>].

505. *Id.*

Journal, Verizon has 98.9 million wireless customers and 22.2 million landline customers; AT&T has 107.3 million wireless customers and 31.2 million landline customers; and Sprint has 55 million customers in total.⁵⁰⁶ In short, the program monitors hundreds of millions of people.

As for the type of information obtained, the FISC order requests that the telephone service providers give the government all “call detail information,” a term that is defined by regulatory provision as: “Any information that pertains to the transmission of specific telephone calls, including, for outbound calls, the number called, and the time, location, or duration of any call and, for inbound calls, the number from which the call was placed, and the time, location, or duration of any call.”⁵⁰⁷ The FISC order further directs that the company provide “session identifying information,” such as originating and terminating number, International Mobile Subscriber Identity number, and the International Mobile station Equipment Identity number.⁵⁰⁸ As Edward Felten, a Professor of Computer Science at Princeton University, recently explained to the Senate Judiciary Committee:

These are unique numbers that identify the user or device that is making or receiving a call. Although people who want to evade surveillance can make it difficult to connect these numbers to their individual identities, for the vast ma-

506. *Id.*

507. 47 C.F.R. § 64.2003 (2012). Senior intelligence officials have repeatedly asserted that, although they have the authority to collect GPS data, and have in the past, they are not currently doing so under the Section 215 telephony metadata program. See, e.g., *Joint Statement for the Record of Director of National Intelligence James Clapper and General Keith Alexander Before the the S. Comm. on the Judiciary*, 113th Cong. (2013); Siobhan Gorman & Julian E. Barnes, *Officials: NSA Doesn't Collect Cellphone-Location Records*, WALL ST. J., June 16, 2013, <http://onlwsj.com/13MnSsp>, [<http://perma.cc/0ogJY4FNywU>].

508. *In re Application of the FBI for an Order Requiring the Production of Tangible Things from Verizon Bus. Network Svcs.*, Secondary Order, BR 13-80, at 2 (FISA Ct. Apr. 25, 2013), available at <http://www.theguardian.com/world/interactive/2013/jun/06/verizon-telephone-data-court-order?guni=Article:in%20body%20link>, [<http://perma.cc/V9Z6-TZAJ>].

jority of ordinary Americans these numbers can be connected to the specific identity of a person.⁵⁰⁹

The FISC order also directs the company to provide trunk identifier information. This data traces the route a telephone call takes, in the process establishing the location of the people taking part in the conversation.⁵¹⁰

What can be done with this information is a significantly deeper intrusion on Americans' right to privacy than was at issue in *Smith*. As Felten explains, "Telephony metadata is easy to aggregate and analyze because it is, by its nature, *structured data*."⁵¹¹ Sophisticated data-mining and link-analysis programs can be used to then analyze this information, and it can do so more quickly, deeply, and cheaply than in the past. Even the amount of data that can be retained for such analysis is of a radically different scale than was conceivable in 1979.

From this information, the government can determine patterns and relationships, such as personal details, habits, and behaviors, that U.S. citizens had no intention or expectation of sharing.⁵¹² The government can also obtain content. Felten writes:

[C]ertain telephone numbers are used for a single purpose, such that any contact reveals basic and often sensitive information about the caller. Examples include support hotlines for victims of domestic violence and rape. Similarly, numerous hotlines exist for people considering suicide, including specific services for first responders, veterans, and gay and lesbian teenagers. Hotlines exist for sufferers of various forms of addiction, such as alcohol, drugs, and gambling. Similarly, inspectors general at practically every federal agency—including the NSA—have hotlines through which misconduct, waste, and fraud can be reported, while numerous state tax agencies have dedicated hotlines for reporting tax fraud. Hotlines have also been established to report hate crimes, arson, illegal firearms and child abuse The phone records indicating that someone called

509. *Hearing on Continued Oversight of the Foreign Intelligence Surveillance Act Before the S. Comm. on the Judiciary*, 113th Cong. 3 (2013) (written testimony of Edward W. Felten, Professor, Princeton Univ.).

510. *Id.*

511. *Id.* at 4 (noting that the numbers are in predictable formats, as is the time and date information, and contrasting telephony metadata to content).

512. *Id.* at 5.

a sexual assault hotline or a tax fraud hotline will of course not reveal the exact words that were spoken during those calls, but phone records indicating a 30-minute call to one of these numbers will still reveal information that virtually everyone would consider extremely private.⁵¹³

Even if U.S. citizens wanted to opt out of having this information collected, it would be virtually impossible to do so. There have, for instance, been advances in encryption. But these technologies all revolve around content—not metadata. Although some technologies are focused on metadata, these are not sufficiently advanced to allow for real-time communication.⁵¹⁴ The only option is therefore not to use a telephone. The cost of doing so, however, would lean towards divesting oneself of a role in the modern world—impacting one’s social relationships, employment, and ability to conduct financial and personal affairs.

Notably, all of these considerations are focused on telephony metadata. But the logic of the government’s argument, as applied to metadata generally, has virtually no limit. One could equally argue that all financial flows, Internet usage, and e-mail exchanges are relevant to ongoing terrorism investigations under section 215. Almost all forms of metadata could be at stake.

Americans have contractual relationships with myriad corporate entities, to whom they have entrusted parts of their lives, such as friendships, correspondence, buying patterns, and financial records. Creating a contractual relationship with Safeway, however, to gain access to reduced prices for food, is something different in kind from divulging to the U.S. government that you keep kosher, help to support your mother, and attend synagogue. Americans reasonably expect that their movements, decisions, and communications will not be recorded and analyzed by the intelligence agencies.

C. *Judicial Tension: Trespass and Katz’s Reasonable Expectation of Privacy*

In *Katz v. United States*, the Court replaced the previous trespass doctrine with one based on a reasonable expectation of

513. *Id.* at 8–9 (internal footnotes omitted).

514. *Id.* at 7–8.

privacy. The Court explained, “The fact that the electronic device employed to” record Katz’s conversation “did not happen to penetrate the wall of the phone booth can have no constitutional significance.”⁵¹⁵ For the Court, the Constitution protected electronic violations, as much as physical intrusions, into space otherwise protected by the Fourth Amendment.

Katz itself was an effort by the Court to come to terms with new technologies. Since that time, tension has emerged and now marks a split on the Court between those who consider Fourth Amendment incursions in terms of physical trespass, and those who adopt the reasoning of *Katz* more broadly. Thus, a series of cases involving areas such as thermal imaging,⁵¹⁶ GPS devices,⁵¹⁷ and highly-trained dogs,⁵¹⁸ divide along these lines, with one Justice (Sotomayor) siding alternately with one side or the other. Regardless of which approach one adopts, however, the bulk collection of Americans’ metadata runs afoul of the Fourth Amendment.

In the realm of trespass, the program authorized under Section 215 amounts to a general warrant—which was the very definition of an unreasonable search and seizure at the time of the founding. It was to prohibit general warrants, and thereby to gain the support of anti-Federalists for the fledgling Constitution, that James Madison wrote the Fourth Amendment and introduced it into Congress in 1789 as part of the Bill of Rights.⁵¹⁹ The telephony metadata program, moreover, amounts to a digital trespass on citizens’ private lives. The application of *Katz*’s reasonable expectation of privacy test, albeit via a different route, reaches a similar conclusion: that is, the telephony metadata collection program falls within Fourth Amendment protections.

1. *The Prohibition on General Warrants*

At the time of the founding, English courts rejected general warrants. A different standard, however, marked the crown’s

515. *Katz v. United States*, 389 U.S. 347, 353 (1967).

516. *Kyllo v. United States*, 533 U.S. 27 (2001).

517. *United States v. Jones*, 132 S. Ct. 945 (2012).

518. *Florida v. Jardines*, 133 S. Ct. 1409 (2013); *see also* *Florida v. Harris*, 133 S. Ct. 1050 (2013).

519. *See* Thomas Y. Davies, *Recovering the Original Fourth Amendment*, 98 MICH. L. REV. 547, 693–724 (1999).

treatment of the American colonies. This angered the colonists, who saw themselves, first and foremost, as Englishmen—and therefore deserving of all the rights and privileges accorded to English subjects.

Perhaps the most famous case establishing the right of Englishmen to be free of a general writ dates from November 1762, when King George III's messengers broke into a man's home to execute a warrant issued by the Secretary of State.⁵²⁰ The warrant empowered the king's men "to make strict and diligent search for . . . the author, or one concerned in the writing of several weekly very seditious papers."⁵²¹ The men, who searched John Entick's home for four hours without his consent and against his will, "broke open, and read over, pried into and examined all [of his] private papers [and] books."⁵²² Upon departure, the men seized Entick's documents, charts, pamphlets, and other materials.⁵²³ Chief Justice of the Common Pleas Charles Pratt, First Earl Camden, ruled that both the search and the seizure were unlawful. He explained:

520. *Entick v. Carrington* (1765) 95 Eng. Pep. 807 (K.B.).

521. The full warrant read:

George Montagu Dunk, Earl of Halifax, Viscount Sunbury, and Baron Halifax one of the Lords of his Majesty's Honourable Privy Council, Lieutenant General of His Majesty's Forces, Lord Lieutenant-General and General Governor of the kingdom of Ireland, and principal Secretary of State, etc. these are in His Majesty's name to authorize and require you, taking a constable to your assistance, to make strict and diligent search for John Entick, the author, or one concerned in writing of several weekly very seditious papers, entitled *The Monitor, or British Freeholder*, No 357, 358, 360, 373, 376, 378, 379, and 380, London, printed for J. Wilson and J. Fell in Pater-Noster-Row; which contains gross and scandalous reflections and invectives upon His Majesty's Government, and upon both Houses of Parliament, and him, having found, you are to seize and apprehend, and to bring, together with his books and papers, in safe custody before me to be examined concerning the premises, and further dealt with according to law; in the due execution whereof all mayors, sheriffs, justices of the peace, constables, and other His Majesty's officers civil and military, and all loving subjects whom it may concern, are to be aiding and assisting to you as there shall be occasion; and for so doing this shall be your warrant. Given at St. James's the 6th day of November 1762, in the third year of His Majesty's reign, Duke Halifax. To Nathan Carrington, James Watson, Thomas Ardran, and Robert Blackmore, four of His Majesty's messengers in ordinary.

Id. at 807.

522. *Id.* at 814.

523. *Id.* at 807–08.

Suppose a warrant which is against law be granted, such as no justice of peace, or other magistrate high or low whomsoever, has power to issue, whether that magistrate or justice who grants such warrant, or the officer who executes it, are within the [statute] 24 Geo. 2, c. 44? To put one case . . . suppose a justice of peace issues a warrant to search a house for stolen goods, and directs it to four of his servants, who search and find no stolen goods, but seize all the books and papers of the owners of the house, whether in such a case would the justice of peace, his officers or servants, be within the [statute]?⁵²⁴

Two aspects to the case proved particularly troubling: first, the writ had empowered the crown to seize all documents—not just those of a criminal nature; and, second, no demonstration had been made prior to the search and seizure establishing the probability that Entick was engaged in criminal activity:

The warrant in our case was an execution . . . without any previous summons, examination, hearing the plaintiff, or proof that he was the author of the supposed libels; a power claimed by no other magistrate whatever . . . it was left to the discretion of these defendants to execute the warrant in the absence or presence of the plaintiff, when he might have no witness present to see what they did; for they were to seize all papers, bank bills, or any other valuable papers they might take away if they were so disposed; there might be nobody to detect them.⁵²⁵

The court suggested that since the Glorious Revolution and the restoration of William and Mary to the throne, such powers had been denied to the crown. It was precisely such aggrandizement of power that had led to revolution in the first place. The Chief Justice stated, “we can safely say there is no law in this country to justify the defendants in what they have done; if there was, it would destroy all the comforts of society; for papers are often the dearest property a man can have.”⁵²⁶ The court flatly rejected the use of such general warrants.

What was banned in England, however, became commonplace in the colonies. Resultantly, the use of writs of assistance

524. *Id.* at 814.

525. *Id.* at 817.

526. *Id.* at 817–18.

played a central role in lending speed to the American Revolution. Acting under writs established by Parliamentary statute, officers of the crown had permission to search the homes, papers, and belongings of any person.⁵²⁷ As early as 1660, legislation empowered magistrates to:

[I]ssue out a Warrant to any person or persons thereby enabling him or them with the assistance of a Sheriffe Justice of Peace or Constable to enter into any House in the day time where such Goods are suspected to be concealed, and in case of resistance to breake [sic] open such Houses, and to seize and secure the same goods soe [sic] concealed, And All Officers and Ministers of Justice are hereby required to be aiding and assisting thereunto.⁵²⁸

The writs came to be seen as the worst instrument of arbitrary power, turning colonists against the crown. Their use was part of a general crack-down engineered by British Prime Minister William Pitt, who directed the American colonial governors and royal customs officers to enforce trade and navigation laws more strictly—specifically, to “make the strictest and most diligent Enquiry into the State of this dangerous and ignominious Trade.”⁵²⁹ He ordered that every step authorized by law be taken “to bring all such heinous Offenders to the most exemplary and condign [sic] Punishment.”⁵³⁰

In response to Pitt’s order, the governor of Massachusetts Bay Colony began making use of the writ, prompting Boston merchants to hire James Otis to challenge their constitutionality. In what has become one of the most famous examples of early American legal oration, Otis argued that the writs were

527. Officials could “enter and go into any House, Warehouse, Shop, Cellar, or other Place” to seize goods. M.H. SMITH, *THE WRITS OF ASSISTANCE CASE 1* (1978) (quoting a 1767 measure by Parliament, establishing a new writ of assistance in America).

528. An Act to Prevent Fraudes and Concealments of His Majestyes Customes and Subsidiyes, 12 Car. II, c. 19 (1660); *see also* Act for Preventing Fraudes and Regulating Abuses in his Majestyes Customes, 14 Car. II, c. 11 (1662). A good discussion of the early writs of assistance is located in JOSEPH R. FRESE, *EARLY PARLIAMENTARY LEGISLATION ON WRITS OF ASSISTANCE*, PUBLICATIONS OF THE COLONIAL SOCIETY OF MASSACHUSETTS (1959).

529. Horace Gray, *Writs of Assistance*, in JOSIAH QUINCY, JR., *REPORTS OF CASES ARGUED AND ADJUDGED IN THE SUPERIOR COURT OF JUDICATURE OF THE PROVINCE OF MASSACHUSETTS BAY BETWEEN 1761 AND 1772*, at 407 (Samuel M. Quincy ed. 1865).

530. *Id.* at 408.

contrary to “the fundamental principles of law.”⁵³¹ Scholars hail Otis’s argument in the case as helping “to lay the foundation for the breach between Great Britain and her continental colonies.”⁵³² As A.J. Langguth observed, at the Writs of Assistance trial, “James Otis stood up to speak, and something profound changed in America.”⁵³³

One of our best accounts of Paxton’s Case comes from John Adams, who was present at the argument and whose mentor, Jeremiah Grindley, the most distinguished member of the bar in Boston, opened the case for the crown.⁵³⁴ In replying to Grindley, Otis stated that his efforts were being made “out of regard to the liberties of the subject.”⁵³⁵ The rights of British subjects were under assault, compelling him to oppose “all such instruments of slavery on the one hand and villainy on the other as this Writ of Assistance is.”

For Otis, the writ was “the worst instrument of arbitrary power.”⁵³⁶ He ignored the crown’s claim of necessity—and current practice—noting that “the writ prayed for in this petition, being general, is illegal.”⁵³⁷ He highlighted four concerns: first, it was universal—in other words, it could be executed by anyone in possession of it; second, it was perpetual in that it indefinitely allowed the holder of the writ to conduct searches; third, no prior evidence of wrongdoing need be involved in its execution; and fourth, there was no requirement to swear to suspicion of wrongdoing or, following execution, to inquire into its exercise. “One of the most essential branches of English liberty

531. NORMAN K. RISJORD, *JEFFERSON’S AMERICA 1760–1815*, at 75 (2d ed. 2002).

532. LAWRENCE HENRY GIPSON, *THE COMING OF THE REVOLUTION, 1763–1777*, at 39 (1954).

533. A.J. LANGGUTH, *PATRIOTS: THE MEN WHO STARTED THE AMERICAN REVOLUTION* 22 (1989).

534. James M. Farrell, *The Child Independence Is Born: James Otis and Writs of Assistance*, in 2 *A RHETORICAL HISTORY OF THE UNITED STATES: SIGNIFICANT MOMENTS IN AMERICAN PUBLIC DISCOURSE* 16 (Stephen E. Lucas, ed. forthcoming); see also *Paxton’s Case of the Writ of Assistance*, in JOSIAH QUINCY, *supra* note 529.

535. Otis’s speech is taken from 2 *THE LEGAL PAPERS OF JOHN ADAMS* 139–44 (L. Kinvin Wroth & Hiller B. Zobel, eds. 1965).

536. *Id.*

537. *Id.*

is the freedom of one's house," Otis opined.⁵³⁸ General warrants would annihilate the privilege associated with that right.

Although the court ruled against Otis, John Adams later wrote that his arguments "breathed into this nation the breath of life."⁵³⁹ On June 12, 1776, the Virginia Constitutional Convention adopted the Virginia Declaration of Rights—a document that deeply influenced the Declaration of Independence, as well as other states' constitutions, and became the basis for the Bill of Rights—without which, the Constitution would never have been ratified.

The Virginia Declaration of Rights stated, *inter alia*, "That general warrants, whereby an officer or messenger may be commanded to search suspected places without evidence of a fact committed, or to seize any person or persons not named, or whose offense is not particularly described and supported by evidence, are grievous and oppressive and ought not to be granted."⁵⁴⁰ The Massachusetts Constitution of 1780 similarly objected to the use of general warrants:

Every subject has a right to be secure from all unreasonable searches and seizures of his person, his houses, his papers, and all his possessions. All warrants, therefore, are contrary to this right, if the cause or foundation of them be not previously supported by oath or affirmation, and if the order in the warrant to a civil officer, to make search in suspected places, or to arrest one or more suspected persons, or to seize their property, be not accompanied with a special designation of the persons or objects of search, arrest, or seizure; and no warrant ought to be issued but in cases, and with the formalities, prescribed by the laws.⁵⁴¹

The New Hampshire Constitution of 1784 lifted the clause almost verbatim.⁵⁴² The Virginia ratifying convention of 1788

538. *Id.*

539. 10 CHARLES FRANCIS ADAMS, THE WORKS OF JOHN ADAMS 276 (Boston, Little, Brown & Co. 1856).

540. VA. DECL. OF RIGHTS § 10.

541. MASS. CONST. of 1780, pt. 1, art. XIV.

542. N.H. CONST. of 1784, art. XIX ("Every subject hath a right to be secure from all unreasonable searches and seizures of his person, his houses, his papers, and all his possessions. All warrants, therefore, are contrary to this right, if the cause or foundation of them be not previously supported by oath, or affirmation; and if the order in the warrant to a civil officer, to make search in suspected places, or to

made a point to ensure that the subsequent Constitution would include a provision affirming that “every freeman has a right to be secure from all unreasonable searches and siezures [sic] of his person, his papers and his property.”⁵⁴³ New York, in turn, required nearly identical language, as did North Carolina—even as Virginia, New York, and North Carolina all condemned overbroad warrants as “‘therefore’ unreasonable—‘grievous,’ ‘oppressive,’ and ‘dangerous.’”⁵⁴⁴ Consistent with these states’ understandings, James Madison’s first draft of the Fourth Amendment addressed the right of the people “to be secured in their persons, their houses, *their papers, and their other property*, from all unreasonable searches and seizures.”⁵⁴⁵ Madison understood the clause as a ban against general warrants.⁵⁴⁶

In 1886 the Supreme Court recognized the importance of the writs and the Founders’ rejection of the same as encapsulated in the Fourth Amendment:

In order to ascertain the nature of the proceedings intended by the Fourth Amendment to the Constitution under the terms “unreasonable searches and seizures,” it is only necessary to recall the contemporary or then recent history of the controversies on the subject, both in this country and in England. The practice had obtained in the colonies of issuing writs of assistance to the revenue officers, empowering them, in their discretion, to search suspected places for smuggled goods, which James Otis pronounced “the worst instrument of arbitrary power, the most destructive of English liberty, and the fundamental principles of law, that ever

arrest one or more suspected persons, or to seize their property, be not accompanied with a special designation of the persons or objects of search, arrest, or seizure; and no warrant ought to be issued but in cases, and with the formalities prescribed by the laws.”).

543. Akhil Reed Amar, *The Fourth Amendment, Boston, and the Writs of Assistance*, 30 SUFFOLK U. L. REV. 53, 68 (1996) (quoting EDWARD DUMBAULD, *THE BILL OF RIGHTS AND WHAT IT MEANS TODAY* 184 (1957)).

544. *Id.* at 68 (quoting DUMBAULD, *supra* note 543, at 184, 191, 200–01).

545. *Id.* (quoting DUMBAULD, *supra* note 543, at 207 (emphasis added)). Note that the historical antecedent suggests a broad reading of the “persons, houses, papers, and effects” language of the Fourth Amendment.

546. See Davies, *supra* note 519, at 555; see also N. LASSON, *THE HISTORY AND DEVELOPMENT OF THE FOURTH AMENDMENT TO THE UNITED STATES CONSTITUTION* 103 (1937); Robert M. Bloom, *Warrant Requirement – The Burger Court Approach*, 53 U. COLO. L. REV. 691, 692 (1982).

was found in an English law book;" since they placed "the liberty of every man in the hands of every petty officer." This was in February, 1761, in Boston, and the famous debate in which it occurred was perhaps the most prominent event which inaugurated the resistance of the colonies to the oppressions of the mother country. "Then and there," said John Adams, "then and there was the first scene of the first act of opposition to the arbitrary claims of Great Britain. Then and there the child Independence was born."⁵⁴⁷

The Court acknowledged the importance of Lord Camden's decision in *Entick v. Carrington*:

[Camden's] great judgment on that occasion is considered as one of the landmarks of English liberty. It was welcomed and applauded by the lovers of liberty in the colonies as well as in the mother country. It is regarded as one of the permanent monuments of the British Constitution, and is quoted as such by the English authorities on that subject down to the present time.⁵⁴⁸

It was precisely general warrants that the Framers meant when referring to unreasonable searches and seizures.⁵⁴⁹

Throughout U.S. history, the Supreme Court has continued to recognize the special role played by general warrants and writs of assistance in shaping the contours of the Fourth Amendment. In 1980, the Court recognized that it was "familiar history that indiscriminate searches and seizures conducted under the authority of 'general warrants' were the immediate evils that motivated the framing and adoption of the Fourth Amendment."⁵⁵⁰ General warrants were presumptively unreasonable.

Consistent with this reading, Professor Akhil Amar, inquiring as to what the warrant clause means—and what the relationship is between it and the earlier reasonableness clause—suggests that "broad warrants—warrants that fail to meet the various specifications of clause two—are inherently unreasonable under clause one."⁵⁵¹ Such a general warrant would immunize the officer who carried it out from a subsequent tres-

547. *Boyd v. United States*, 116 U.S. 616, 624–25 (1886).

548. *Id.* at 626.

549. *Id.* at 626–27.

550. *Payton v. New York*, 445 U.S. 573, 583 (1980).

551. See Amar, *supra* note 543, at 60.

pass suit.⁵⁵² In the case of *Entick v. Carrington*, “Armed with sweeping warrants issued by executive officials, various government henchmen broke into Englishmen’s houses, searched their papers, arrested their persons, and rummaged through their effects, in hopes of finding” wrongdoing.⁵⁵³

Professor Thomas Davies similarly recognizes that “[t]he historical statements about search and seizure” in the Fourth Amendment “focused on condemning general warrants. In fact, the historical concerns were almost exclusively about the need to ban house searches under general warrants.”⁵⁵⁴ Evidence suggests that “unreasonable searches and seizures” was a proxy for “the inherent illegality of any searches or seizures that might be made under general warrants.”⁵⁵⁵ Davies posits that the reason the Framers even bothered “to adopt constitutional bans against general warrants in light of the apparent consensus that the general warrant was illegal at common law” was because of genuine concern that Congress might endanger the right in the future.⁵⁵⁶

The FISC Order authorizing the telephony metadata program is a general warrant. It authorizes the government to rummage through our papers and effects in the hope of finding wrongdoing. There is no previous suspicion of criminal activity. Almost none of the information obtained relates to illegal behavior.

It matters little whether one stores one’s papers in a filing cabinet in one’s den, or places all financial documents in the iCloud—the digital equivalent, in modern times, of a filing cabinet. Sheer volume of information requires individuals to arrange for storage of everything from medical records to family photos. E-mail, in turn, holds our correspondence—papers that we place on a server with a company with whom we have a contractual relationship. Banking records may be accessible over the Internet. These are our modern day equivalents of the papers and effects held by Entick in his home.

552. *Id.*

553. *Id.* at 65.

554. Davies, *supra* note 519, at 551.

555. *Id.*

556. *Id.* at 657.

In considering the case of *Entick v. Carrington*, Lord Camden wrote, “The great end for which men entered into society was to secure their property.”⁵⁵⁷ He continued, “By the laws of England, every invasion of private property, be it ever so minute, is a trespass.” Camden added:

Papers are the owner’s goods and chattels; they are his dearest property, and are so far from enduring a seizure that they will hardly bear an inspection . . . where private papers are removed and carried away, the secret nature of those goods will be an aggravation of the trespass, and demand more considerable damages in that respect.⁵⁵⁸

Allowing the government to obtain bulk metadata is the equivalent of a digital trespass on what Justice Brandeis referred to as the “privacies of life.”⁵⁵⁹ Not only does the government gain penetrating insight into our private affairs, but it does so to a degree that even those engaged in the activity itself do not realize. That it is an electronic trespass, and not a physical one, matters naught. Brandeis explained, “It is not the breaking of his doors, and the rummaging of his drawers, that constitutes the essence of the offence; but it is the invasion of his indefeasible right of personal security, personal liberty and private property . . .”⁵⁶⁰ The digital trespass in which the NSA is engaging is not supported by probable cause. It is not supported by reasonable suspicion. No suspicion of any wrongdoing whatsoever is contemplated by the collection of records. It is the equivalent of a general warrant and, as such, is odious to the Fourth Amendment.

2. *Search of Metadata and the Reasonable Expectation of Privacy*

In recent Fourth Amendment cases considering new technologies, a schism has appeared in the Court between adopting an approach based on traditional concepts of trespass, and examining the facts from the vantage of the reasonable expectation of privacy—a higher bar adopted in 1967 as a way of augmenting the Court’s previous reliance on physical space.

557. (1765) 19 Howell’s State Trials 1029 (C.P.) 1066.

558. *Id.*

559. *Olmstead v. United States*, 277 U.S. 438, 473 (1928) (Brandeis, J., dissenting).

560. *Id.* at 474–75.

In *United States v. Jones*,⁵⁶¹ the Court considered a case involving 28-day surveillance.⁵⁶² The government obtained a search warrant permitting it to place a Global-Positioning System (GPS) tracking device on a car registered to the wife of a suspected drug dealer.⁵⁶³ The day after the warrant expired, agents installed the device and followed the car's movements for nearly a month.⁵⁶⁴ Information thus obtained allowed the government to indict Antoine Jones and others on drug trafficking conspiracy charges.⁵⁶⁵ The Supreme Court held that attaching the GPS device to the car and tracing its movements amounted to a search within the meaning of the Fourth Amendment.⁵⁶⁶

This case is important for determining the constitutionality of the telephony metadata program in three important ways. First, it recognized that *Katz*'s reasonable expectation of privacy test did not supplant the rights in existence at the time the Fourth Amendment was forged. Justice Scalia, writing for the Court, explained:

It is important to be clear about what occurred in this case: The government physically occupied private property for the purpose of obtaining information. We have no doubt that such a physical intrusion would have been considered a "search" within the meaning of the Fourth Amendment when it was adopted.⁵⁶⁷

Justice Scalia cited *Entick v. Carrington*, noting that the Court had described it as a "'monument of English freedom' 'undoubtedly familiar' to 'every American statesman' at the time the constitution was adopted, and considered to be 'the true and ultimate expression of constitutional law' with regard to search and seizure."⁵⁶⁸ For Justice Scalia, and for the Court, the reasonable expectation of privacy test was of no consequence: "At bottom, we must 'assur[e] preservation of that degree of

561. 132 S. Ct. 945 (2012).

562. *Id.* at 946.

563. *Id.*

564. *Id.*

565. *Id.*

566. *Id.* at 949.

567. *Id.*

568. *Id.*

privacy against government that existed when the Fourth Amendment was adopted.”⁵⁶⁹

Just as the Court eschewed *Katz v. United States* as being inapposite for consideration of the rights that existed when the Fourth Amendment was adopted, it would be equally inapposite to dismiss the Fourth Amendment’s rejection of general warrants. “[A]t a minimum,” Justice Scalia wrote, the “18th-century guarantee against unreasonable searches . . . must provide . . . the degree of protection it afforded when it was adopted.”⁵⁷⁰ The concept of a general warrant and the Court’s conception of trespass are, as previously noted, historically connected. The reason that general warrants were rejected at the time of the Founding was because they provided a carte blanche to the government to trespass at will upon one’s property and to search through one’s papers and effects without any reasonable suspicion.

The second point to draw out of *Jones* is that what can be considered a shadow majority appears to recognize that changed circumstances exist, so as to augment the need for new privacy protections. At least five Justices indicated unease with the intrusiveness of modern technology in light of changed times, offering in the process different aspects of a mosaic theory of privacy. Justice Alito, joined by Justice Ginsburg, Justice Breyer, and Justice Kagan, suggested that in most criminal investigations, long-term monitoring “impinges on expectations of privacy.”⁵⁷¹ The nature of new technologies mattered:

Recent years have seen the emergence of many new devices that permit the monitoring of a person’s movements. In some locales, closed-circuit television video monitoring is becoming ubiquitous. On toll roads, automatic toll collection systems create a precise record of the movements of motorists who choose to make use of their convenience. Many motorists purchase cars that are equipped with devices that permit a central station to ascertain the car’s location at any time so that roadside assistance may be provided if needed and the car may be found if it is stolen.⁵⁷²

569. *Id.* at 947.

570. *Id.* at 953.

571. *Id.* at 964 (Alito, J., concurring).

572. *Id.* at 963.

Unlike in the past, the daily business of living one's life creates a digital record with privacy implications. "Perhaps most significant," Justice Alito added, "cell phones and other wireless devices now permit wireless carriers to track and record the location of users—and as of June 2011, it has been reported, there were more than 322 million wireless devices in use in the United States."⁵⁷³ Before computers, practicality proved one of the greatest protectors of individual privacy. It was difficult and expensive to conduct long-term surveillance. But technology has changed the equation. The government now is more able to engage in long-term surveillance; but though relatively short-term monitoring of individuals' movements in public space might be consistent with the Fourth Amendment, "the use of longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy."⁵⁷⁴

Justice Sotomayor went one step further, calling into question the entire basis for third party doctrine. Specifically, in light of the level of intrusiveness represented by modern technology, "it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties."⁵⁷⁵ Sotomayor pointed out:

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 the 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.⁵⁷⁶

She added, "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."⁵⁷⁷

573. *Id.*

574. *Id.* at 964.

575. *Id.* at 957 (Sotomayor, J., concurring).

576. *Id.*

577. *Id.*

The third point to draw from *Jones* reflects the growing tension between trespass and the *Katz* test, as applied to new and emerging technologies—and the increasingly consistent results reached by the Court, regardless of which approach is adopted. Thus, although Justice Sotomayor sided with the majority on trespass grounds, she still embraced the same result as a product of the application of *Katz*.

Jones was not the first manifestation of this tension in light of new and emerging technologies. In *Kyllo v. United States*,⁵⁷⁸ the Court considered whether thermal scanning conducted outside of a target's home constituted a search within the meaning of the Fourth Amendment.⁵⁷⁹ Agents, having picked up a heat signature that suggested that grow lights were being used inside the target's garage, used the information to obtain a search warrant which, when executed, revealed several marijuana plants. As in *Jones*, the concept of trespass figured largely in the decision.⁵⁸⁰

In *Kyllo*, the Court held that where the government employed a device, not in general public use, to uncover details inside a home that otherwise could only be uncovered via physical intrusion, such surveillance constituted a search within the meaning of the Fourth Amendment and was thus presumptively unreasonable without a warrant.⁵⁸¹ As in *Jones*, Justice Scalia delivered the opinion of the Court: "It would be foolish to contend," he wrote, "that the degree of privacy secured to citizens by the Fourth Amendment has been entirely unaffected by the advance of technology."⁵⁸² The question the Court confronted was "what limits there are upon this power of technology to shrink the realm of guaranteed privacy."⁵⁸³ In this equation, Scalia suggested, homeowners should not be left to "the mercy of advancing technology."⁵⁸⁴ The Fourth Amendment, if nothing else, drew a bright line at the curtilage of the home.

578. 533 U.S. 27 (2001).

579. *Id.* at 29.

580. *Id.* at 31–32.

581. *Id.* at 40.

582. *Id.* at 33–34.

583. *Id.*

584. *Id.* at 35.

The dissent, written by Justice Stevens and joined by Chief Justice Rehnquist, Justice O'Connor, and Justice Kennedy, considered the heat signature of the plant to be in the public domain.⁵⁸⁵ For the dissenters, the case did not turn on the question of whether there was search or a seizure inside a home without a warrant, but rather on the application of plain view doctrine:

Indeed, the ordinary use of the senses might enable a neighbor or passerby to notice the heat emanating from a building, particularly if it is vented, as was the case here. Additionally, any member of the public might notice that one part of a house is warmer than another part or a nearby building if, for example, rainwater evaporates or snow melts at different rates across its surfaces. Such use of the senses would not convert into an unreasonable search if, instead an adjoining neighbor allowed an officer onto her property to verify her perceptions with a sensitive thermometer.⁵⁸⁶

For the dissent, applying *Katz*, there was no reasonable expectation of privacy in heat emissions located outside of the home. At the same time, however, the dissent was careful not to limit Fourth Amendment protections to homes themselves: "If such equipment did provide its user with *the functional equivalent of access to a private place*—such as, for example, the telephone booth involved in *Katz*, or an office building—then the rule should apply to such an area as well as a home."⁵⁸⁷ The collection of telephony metadata can be considered in both senses—as a digital trespass within the private sphere (and thus consistent with the majority opinion), as well as a violation of the reasonable expectation of privacy that attends "the functional equivalent of access to a private place," such as one's filing cabinet or personal telephone records.⁵⁸⁸

Electronic recordkeeping has become integral to the conduct of life in the twenty-first century. Electronic communications have now assumed a vital role with regard to social, political, economic, and other activity. As a new technology, embedded in our social structure, it is on a par with the role of the telephone that the Court considered in *Katz*:

585. *Id.* at 41 (Stevens, J., dissenting).

586. *Id.* at 43.

587. *Id.* at 48–49.

588. *Id.*

One who occupies [a phone booth], shuts the door behind him, and pays the toll that permits him to place a call is surely entitled to assume that the words he utters into the mouthpiece will not be broadcast to the world. *To read the Constitution more narrowly is to ignore the vital role that the public telephone has come to play in private communication.*⁵⁸⁹

Whatever role telephones played in 1967, their integration into society has only deepened in the intervening years. Electronic communications have come to play a vital role not just in social interactions, but in conducting all of one's private affairs. That we contract with private companies to ensure careful treatment of this information, that we use passwords to access our telephone, banking, and financial records online, and that we limit access to this information, is the equivalent of shutting the door of the phone booth.

The courts are beginning to recognize privacy interests in this new, electronic sphere. In 2010, for instance, in *United States v. Warshak*, the Sixth Circuit held that the government had violated Warshak's Fourth Amendment rights when it obtained e-mail content from Warshak's internet service provider, absent a warrant based on probable cause.⁵⁹⁰ The court noted that Warshak had a reasonable expectation of privacy in the e-mail he had stored with an ISP.⁵⁹¹

The amount of information that computers can hold makes them different in kind. In 2011, the Ninth Circuit considered the search of a computer at the border.⁵⁹² The dissent noted:

Computers store libraries' worth of personal information, including substantial amounts of data that the user never intended to save and of which he is likely completely unaware (for example, browsing histories and records of deleted files in unallocated space). Computers offer "windows into [our] lives far beyond anything that could be, or would be, stuffed into a suitcase for a trip abroad."⁵⁹³

589. *Katz v. United States*, 389 U.S. 347, 352 (1967) (emphasis added).

590. *United States v. Warshak*, 631 F.3d 266 (6th Cir. 2010).

591. *Id.*

592. *United States v. Cotterman*, 637 F.3d 1068 (9th Cir. 2011) (Fletcher, J., dissenting).

593. *Id.* at 1085–86 (internal citations omitted).

For the dissent, particularized suspicion was necessary to perform such searches because individuals have a reasonable expectation of privacy in their electronic files.

Most recently, the Supreme Court has confronted cases involving the use of drug-sniffing dogs. In *Florida v. Jardines*,⁵⁹⁴ the Court held that the use of a narcotics dog outside a home was a “search” within the meaning of the Fourth Amendment.⁵⁹⁵ Once again, Justice Scalia authored the opinion, in which he resolved the question solely on property rights grounds.⁵⁹⁶ The act of placing the dog on the front porch, to conduct a forensic search of someone’s home, constituted a search.⁵⁹⁷ The trespass in question thus proved sufficient to find the act unconstitutional.⁵⁹⁸ The majority did not need to reach the question of whether the sniff also violated the suspect’s reasonable expectation of privacy.⁵⁹⁹

Although the Court did not rule on whether the officers had violated *Jardines*’ expectation of privacy under *Katz*, Justice Elena Kagan offered a concurring opinion in which she noted that, instead of under a property rubric, she “could just as happily have decided [the case] by looking to *Jardines*’ privacy interests.”⁶⁰⁰ For Kagan, law enforcement would have been equally outside the bounds of the Constitution for standing in a space adjacent to one’s dwelling and searching for evidence with impunity. Kagan noted the relationship between the two approaches:

It is not surprising that in a case involving a search of a home, property concepts and privacy concepts should so align. The law of property ‘naturally enough influence[s]’ our ‘shared social expectations’ of what places should be free from governmental incursions.⁶⁰¹

Kagan’s concurrence in *Jardines*, like the dissent’s acknowledgement of *Katz* in *Kyllo*, and Justice Sotomayor’s concurrence in *Jones*, signals a convergence between Justice Scalia and oth-

594. 133 S. Ct. 1409 (2013).

595. *Id.* at 1417–18.

596. *Id.* at 1415–17.

597. *Id.* at 1416.

598. *Id.* at 1417–18.

599. *Id.* at 1417.

600. *Id.* at 1418 (Kagan, J., concurring).

601. *Id.*

ers on the Court as to the existence of mutually-reinforcing spheres protecting U.S. citizens—in the face of new technologies—from undue government interference. This is precisely the space occupied by the bulk collection of U.S. citizens' telephony records. Under either approach, the program, and similarly situated bulk collections of U.S. citizens' records, violates the Fourth Amendment.

D. The Proverbial Needle in the Haystack

We live in an age in which individual actors have the capability and the intent to harm U.S. national security. Such persons may be tied to state actors, the traditional target of U.S. intelligence activities, or they may not. They may be acting as part of a multi-national network, they may be acting on behalf of a domestic group, or they may simply have a grudge against the United States or its people. The potential construction, dissemination, and use of weapons of mass destruction—such as biological weapons, nuclear devices, cyber attack, or conventional force used against critical infrastructure targets—by such persons changes the equation in terms of how the state must act to protect its interests. It must try to anticipate aggression from state actors, of course, but it must also try to anticipate action from non-state actors and individuals.

With such non-traditional threats in mind, proponents of the telephony metadata program have argued that to find threats, intelligence agencies must first obtain, and then mine, all individuals' data. The analogy that has been suggested is that intelligence agencies must first build a haystack, in order to find the proverbial needle. The assumptions underlying this model are that all individuals potentially present a threat, and that the threat from individuals can only be identified and understood in the context of all the data.

For constitutional purposes, the argument continues, it is not a search within the meaning of the Fourth Amendment to build the haystack. This only occurs once someone starts sifting through the hay to find the needle. A further nuance in this argument suggests that, to the extent that the creation of the haystack is being accomplished through technology and automation, and no human being is involved, the building of the haystack—and even the analysis of the data—is outside the confines of the Fourth Amendment.

In its 2011 report to Congress, for instance, the Department of Justice noted two NSA bulk collection programs in existence: first, the telephony metadata program under Section 215 and, second, the bulk collection of e-mail envelope information under the pen-trap provisions of FISA.⁶⁰² DOJ noted, “Both of these programs operate on a very large scale [REDACTED TEXT] However, as described below, only a tiny fraction of such records are ever viewed by NSA intelligence analysts.”⁶⁰³

There are a number of problems with this argument, the first being (consistent with the argument above) that it is the *collection* of information that brings the bulk collection of information within the meaning of a search for Fourth Amendment purposes—that is, under the reasonable expectation of privacy test, individuals reasonably assume that their movements which are recorded by cell phone towers, and their social interactions, placement in social networks, interests, and possible concerns that emerge from calling records, are not going to be recorded and transmitted to the NSA to be analyzed, queried, stored, and shared with other agencies. This is precisely what sets the NSA surveillance program apart from *Smith v. Maryland*, in which limited information was provided by the carrier to the police. It was on these grounds that in December 2013 Judge Richard Leon held that the NSA collection program is likely unconstitutional.⁶⁰⁴

The strongest counterargument is that offered by Judge Pauley of the Southern District of New York, who asserts that calling data on tens of millions of Americans, and the retention of this data, represented precisely what was settled in *Smith*.⁶⁰⁵ In other words, the data in question is only different in volume, not kind, from what was at stake in *Smith v. Maryland*. That it happens to yield more insight into individuals’ lives matters naught: the key question, instead, is whether it has been provided to a third party. The problem with this analysis is that it ignores the point of inquiring into the reasonableness of the

602. Report on the National Security Agency’s Bulk Collection Programs for USA PATRIOT Act Reauthorization, *supra* note 349, at 1 (detailing the collection of business records under Section 215 and the use of pen-trap under Section 402).

603. *Id.* at 3.

604. *Klayman v. Obama*, 957 F. Supp. 2d 1, 43–44 (D.D.C. 2013).

605. *ACLU v. Clapper*, 959 F. Supp. 2d 724, 749–52 (S.D.N.Y. 2013).

search. By including both an objective and a subjective standard, the Court allowed for the context and the evolution of technology to be taken into account. In *Jones*, as was considered above, five Justices questioned whether *Smith* continues to be applicable in light of the evolution of technology.

In a recent post arguing against the constitutionality of the NSA bulk metadata collection program, Professor Geoffrey R. Stone, who served on the President's Review Board of the metadata collection program, added yet a further consideration. The costs traditionally associated with traditional pen registers and trap and trace equipment have, in the past, created a barrier to the government's use of the same.⁶⁰⁶ The use of a pen register is time-consuming, fact specific, and costly. As a practical matter, the government can use it in only a handful of situations. The knowledge that the government can use a pen register without probable cause and a warrant therefore has almost no effect on the average person's expectations of privacy or behavior.⁶⁰⁷

The decision to make a telephone call (or not) thus does not turn on the "infinitesimal risk" that the government might have placed a pen or trap on our number.⁶⁰⁸ Technology, however, Stone argues, has changed the calculation.⁶⁰⁹ The government can now do this without any of the efficiency barriers that, in the past, would have prevented us from being placed under surveillance.⁶¹⁰ This was precisely the point that Justice Alito brought out in *Jones* in relation to the use of GPS technologies.⁶¹¹ Technology should not continually erode our traditional expectations of privacy. Stone observes, "Without that principle, the evolution of a 'Big Brother' government could do serious damage to the liberty, privacy and dignitary interests of the individual that are essential to a free society."⁶¹²

606. Geoffrey R. Stone, *Is the NSA's Bulk Telephony Meta-Data Program Constitutional: Part II*, HUFFINGTON POST, Jan. 6, 2014, http://www.huffingtonpost.com/geoffrey-r-stone/is-the-nsas-bulk-telephon_b_4549449.html, [perma.cc/T62W-9PCH].

607. *Id.*

608. *Id.*

609. *Id.*

610. *Id.*

611. *Id.*

612. *Id.*

In the context of the haystack argument, it is important to note here that the previous *absence* of technology performed an important privacy function: It created administrative barriers to impinging on individuals' private lives. The very question of whether or not to build a haystack is a quintessential twenty-first century question. To suggest that there is no privacy implication in building the haystack ignores the important limiting function that lack of technology and resource constraints previously played.

A second problem with the haystack approach is that the Supreme Court has not recognized any "automation exception" to the Fourth Amendment. To the contrary, it is the moment at which the thermal device picks up the heat signature, when the GPS device is placed on the car, and when the dog sniffs the marijuana inside the home that the search has occurred. In *United States v. Karo*,⁶¹³ for instance, a case that turned on the use of a beeper to follow a suspected drug dealer's car, Justice Stevens explained: "The expectation of privacy should be measured from the standpoint of the citizen whose privacy is at stake, not of the government. It is compromised the moment the invasion occurs. A bathtub is a less private area when the plumber is present even if his back is turned."⁶¹⁴ It is the collection of the information that thus represents an intrusion into privacy.

A variant of the haystack argument that suggests that no search occurs until a human being sees the data being collected ignores the fact that this is a government-centric approach. The Fourth Amendment, however, protects individual rights from government intrusion. It is thus *from the individual's perspective* that one must evaluate both the act of trespass and the objective and subjective expectations of privacy (as under *Katz*). And *from the individual's perspective*, it is at the moment the telephony metadata is collected that the search occurs. It would thus matter little if the government mounted cameras inside every American's home, promising not to actually watch the tapes until some future point in time. The act of mounting the camera and recording the information is precisely what constitutes a

613. 468 U.S. 705 (1984).

614. *Id.* at 735.

search, and thus brings such behavior within the protection of the Fourth Amendment.

A third problem with the government's line of reasoning is that it ignores the intercession of human judgment throughout the process. It is a human being that decides to collect the information. Human beings submit applications to FISC, grant applications, and issue primary and secondary orders to collect the data. Human beings program computers to collect information and to collate it. Human beings write the algorithms, replete with inbuilt assumptions and biases, and then decide where the information goes and in what form it will be available for other human beings to see. In short, human beings are involved throughout the process. To represent it otherwise is to ignore the extent to which technology is being used at the behest of government and not in its stead.

In *McCulloch v. Maryland*, Chief Justice Marshall wrote, "We must never forget that it is a constitution we are expounding."⁶¹⁵ Just over a century later, Justice Brandeis recognized that in the intervening time, the Supreme Court had "repeatedly sustained the exercise of power by Congress, under various clauses of that instrument, over objects of which the Fathers could not have dreamed."⁶¹⁶

For Brandeis, the purpose of the Fourth Amendment was to protect the privacies of life:

But "time works changes, brings into existence new conditions and purposes." Subtler and more far-reaching means of invading privacy have become available to the government. Discovery and invention have made it possible for the government, by means far more effective than stretching upon the rack, to obtain disclosure in court of what is whispered in the closet.⁶¹⁷

Justice Brandeis' words proved prescient:

The progress of science in furnishing the government with means of espionage is not likely to stop with wire-tapping. Ways may someday be developed by which the government, without removing papers from secret drawers, can re-

615. *McCulloch v. Maryland*, 17 U.S. (4 Wheat.) 316 (1819).

616. *Olmstead v. United States*, 277 U.S. 438, 472 (1928) (Brandeis, J., dissenting).

617. *Id.* at 473.

produce them in court, and by which it will be enabled to expose to a jury the most intimate occurrences of the home. Advances in the . . . sciences may bring means of exploring unexpressed beliefs, thoughts and emotions. "That places the liberty of every man in the hands of every petty officer" was said by James Otis of much lesser intrusions than these. To Lord Camden, a far slighter intrusion seemed "subversive of all the comforts of society." Can it be that the Constitution affords no protection against such invasions of individual security?⁶¹⁸

The technologies at issue in the bulk collection program invade U.S. citizens' privacy to a degree unprecedented in the past. It was Brandeis that noted, "As a means of espionage, writs of assistance and general warrants are but puny instruments of tyranny and oppression when compared with wiretapping."⁶¹⁹ Yet the wiretapping of a single individual is but an equally "puny instrument" when compared with the wholesale collection and analysis of all communication records.

IV. CONCLUSION

The 1978 Foreign Intelligence Surveillance Act sought to empower the NSA and others to take advantage of new technologies and to engage in necessary foreign intelligence gathering, while preventing the intelligence community from engaging in sweeping surveillance of U.S. citizens. Congress enacted a series of restrictions, requiring that the target of such surveillance be a foreign power, or an agent thereof, insisting that probable cause support such claims, and heightening the protections afforded to the domestic collection of U.S. citizens' information. FISA's expansion gradually brought physical searches, pen registers and trap and trace devices, as well as business records and tangible goods, within its remit. These new authorities retained much of the structure that defined the statute.

The NSA's bulk collection of metadata contradicts the general approach Congress adopted in enacting FISA. The FISC orders lack the particularization required prior to the acquisition of information and the role FISC now plays departs from

618. *Id.* at 474 (footnotes omitted).

619. *Id.* at 476.

that Congress envisioned. The bulk collection program, moreover, violates the statutory language in at least three ways: it does not comport with the requirement that the tangible goods sought “are relevant to an authorized investigation”; it violates the requirement that the information be otherwise obtainable via subpoena duces tecum; and it bypasses the statutory provisions governing pen registers and trap and trace devices. Compounding the illegality of the program are serious constitutional concerns. The FISC order governing the telephony metadata program amounts to a general warrant, which the Fourth Amendment precludes. The government’s efforts to save the program on grounds of third party doctrine are unpersuasive in light of the unique context of *Smith v. Maryland*, new technologies, and changed circumstances. Growing tension between trespass doctrine and Katz’s reasonable expectation of privacy, as applied to new technologies, suggests that under either approach, the telephony metadata program falls outside constitutional bounds.

There are a number of steps that could be taken as part of a comprehensive FISA reform, to address the shortcomings noted in this Article. First, and most importantly, to comply with constitutional demands, the administration, the courts, or Congress needs to bring the bulk collection of U.S. persons’ metadata under Section 215 to an end. Second, to strengthen FISC’s ability to respond to applications, a number of judicial reforms could be adopted. Foremost on this list is the introduction of adversarial counsel.

In some sense it is inevitable that FISC opinions would extend beyond the original role envisioned by the court (i.e., granting orders), to issuing memorandum opinions. Like all courts, FISC must interpret statutory language and constitutional requirements, in order to apply the law to particular circumstances. Although FISC is not exercising jurisdiction over cases and controversies, it is overseeing a judicial process and, as such, exercising judicial power.⁶²⁰ It is a logical extension of this function that such decisions would then become guidance for similarly situated requests from the Department of Justice and others.

620. U.S. CONST., art. III, § 1 (allocating the judicial power to federal courts, and thus requiring the courts to interpret and to apply federal law).

A high standard of due diligence is recognized and practiced by DOJ's National Security Division (NSD)—an entity particularly aware of its responsibilities in light of *in camera*, *ex parte* proceedings.⁶²¹ It was NSD, for instance, that recognized in January 2009 that the NSA had only been subjecting approximately ten percent of its queries to RAS inspection—and that reported this within a week to FISC.

Nevertheless, for reasons that the Founders and numerous courts in the interim have clearly recognized, the executive branch is hardly a neutral, disinterested observer when its own interests are on the line. Justice Powell explained in *United States v. United States District Court* that the duties and responsibilities of executive officers are “to enforce the laws, to investigate, and to prosecute [T]hose charged with this . . . duty should not be the sole judges of when to utilize constitutionally sensitive means in pursuing their tasks.”⁶²² He underscored the problem: “[U]nreviewed executive discretion may yield too readily to pressures to obtain incriminating evidence and overlook potential invasions of privacy”⁶²³

Allowing contrary views enables the vigorous prosecution of narrow interests, in the process providing FISC with a broader and deeper understanding of the issues at stake. It has taken many scholars by surprise, for instance, that Judge Eagan's August 2013 opinion considers *Smith v. Maryland* as entirely dispositive of the Fourth Amendment question. *United States v. Jones* garners but a footnote, with the opinion omitting any sustained discussion of Fourth Amendment jurisprudence. The importance of adversarial counsel extends beyond merely a constitutional advocate to the potential use of adversarial counsel (with subpoena authorities) to represent corporate and other rights-based interests of U.S. persons. There are a number of ways in which an adversarial process could be created. This

621. See, e.g., *Continued Oversight of the Foreign Intelligence Surveillance Act: Hearing Before the S. Comm. on the Judiciary*, 113th Cong. (2013) (statement of Carrie F. Cordero, Director of National Security Studies, Georgetown University Law Center), available at <http://scholarship.law.georgetown.edu/cong/116>, [perma.cc/7UYT-5WUT].

622. 407 U.S. 297, 317 (1972).

623. *Id.*

is a matter for policy debate. That one is needed, from a legal and constitutional perspective, is clear.

Another alteration that would strengthen FISC's hand would be to provide the court with the technical expertise required to allow it to ensure that the minimization and other procedures it requires are actually followed by the executive branch. As the multiple noncompliance incidents suggest, simply leaving it to the NSA to self-report creates a gap between what is legally required and what occurs in practice. Having deeper insight into the technologies is critical. There is something fundamentally disturbing about FISC simply trusting the executive branch to police its own operations. History, certainly, has taught us the danger of proceeding in this manner.

Yet, further alterations that may address some of FISC's shortcomings relate to substantive changes to the law. Untying the court's hands, for instance, with regard to whether or not certain orders should be granted would help to respond to the critique that the court has such a high rate of acceptance of applications. It is Congress, at least in relation to Section 215, that imposed these limits on FISC. Removing these, and making other statutory changes, such as restoring the prior targeting requirement, heightening protections for U.S. persons, adding "and material" after "relevant," narrowing the definition of "foreign intelligence" to exclude "foreign affairs," and requiring the government to demonstrate past effectiveness prior to renewal orders, would further strengthen the role that FISC could play in overseeing foreign intelligence gathering.

In sum, myriad changes could be put into place to allow the government to take advantage of new technologies, to counter national security threats, and to ensure that the provisions operate in accordance with the U.S. Constitution.⁶²⁴ In the interim, both Congress and the courts have a role to play in insisting that the executive branch operates within statutory and constitutional constraints.

624. As a follow-on to this Article, I construct a taxonomy for potential FISA reforms in Laura K. Donohue, *FISA Reform*, 10 ISJLP (forthcoming 2014), available at <http://scholarship.law.georgetown.edu/cgi/viewcontent.cgi?article=2327&context=facpub>, [perma.cc/NS93-R535].