Remarks prepared for the Oct. 2, 2013 Hearing on
Continued Oversight of the Foreign Intelligence Surveillance Act
Senate Committee on the Judiciary

Professor Laura K. Donohue
Georgetown Law

I. INTRODUCTION

Congress introduced the 1978 Foreign Intelligence Surveillance Act to make use of new technologies and to enable the intelligence community to obtain information vital to U.S.

national security, while preventing the National Security Agency 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 the Cold War and the rapid expansion in communications technologies.

Congress purposefully 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, the Foreign Intelligence Surveillance Act gradually expanded over time to incorporate physical searches, pen registers and trap and trace, and business records and tangible goods. The addition of these provisions took place within the same general framing that Congress had adopted in enacting the legislation in the first place.

Documents related to the recently revealed telephony metadata program, conducted under the auspices of the Foreign Intelligence Act and its subsequent amendments, suggests that the National Security Agency is now interpreting the statutory provisions in a manner directly contrary to Congress' intent. It reflects neither the particularization required by Congress prior to acquisition of information, nor the role anticipated by Congress for the Foreign Intelligence Surveillance Court and Court of Review.

The specific legal reasoning offered in defense of the program, moreover, violates the statutory language in three important ways: (a) it contradicts the requirement the records sought "are relevant to an authorized investigation"; (b) it violates the statutory provision that requires that information sought could be obtained via subpoena duces tecum; and (c) it bypasses the statutory framing for pen registers and trap and trace devices. In addition, the program raises serious constitutional concerns. The FISC order amounts to a general warrant, which the Fourth Amendment is designed to preclude. Efforts by the government to save the program on grounds of third party doctrine are similarly unpersuasive in light of the unique circumstances of *Smith v. Maryland*, new technologies, and changed circumstances. An end to the telephony metadata program and FISA reform are necessary to bring surveillance operations and emerging technologies within the bounds of the Constitution.

II. ORIGINS OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT

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 deeply concerning domestic surveillance operations, prompting Congress to pass the Foreign Intelligence Surveillance Act.

A. Initial Revelations

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 American citizens.[1] 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

[1] Christopher H. Pyle, *CONUS Intelligence: The Army Watches Civilian Politics*, WASHINGTON MONTHLY, Jan. 1, 1970, at 4, *reproduced in* 91 CONG. REC. 2227-2231 (1970).

subsequently published.[2] 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.[3] On December 6, 1973, Stern filed a story that ran on the NBC Nightly News, detailing extensive domestic surveillance and disruption undertaken by the FBI for national security purposes.[4]

Following these initial disclosures, in 1974 Seymour M. Hersh, an investigative reporter, published a detailed report in the *New York Times* that immediately captured public attention. The article stated 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."[5] Intelligence files on more than 10,000 Americans – including members of Congress – had been maintained by a special unit that reported directly to the Director of Central Intelligence.[6] 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."[7] One official reported that the requirement to keep files on U.S. citizens stemmed, in part, from the so-called Huston plan.[8] 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.[9]

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."[10] 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.

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.[11]

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.[12] The Republican leadership in the Senate chose

---

[2] *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.

[3] Memorandum from C.D. Brennan to W.C. Sullivan (Apr. 27, 1971); Letter from FBI headquarters to All SAC's (Apr. 28, 1971), *cited in* SUPPLEMENTARY DETAILED STAFF REPORTS ON INTELLIGENCE ACTIVITIES AND THE RIGHTS OF AMERICANS, BOOK III: FINAL REPORT OF THE SELECT COMMITTEE TO STUDY GOVERNMENTAL OPERATIONS WITH RESPECT TO INTELLIGENCE ACTIVITIES, S. REP NO. 94-755, at 3 (1976) *available at* http://archive.org/stream/finalreportofsel03unit#page/n3/mode/2up.

[4] 91 CONG. REC. 26,329 (1970).

[5] 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.

[6] *Id.*

[7] *Id.*

[8] *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.

[9] *Id.* at 26.

[10] National Security Act of 1947 § 104A(d)(1) (2013).

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

[12] *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).

legislators representing a range of views within their party, as did the Democratic leadership.[13] 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.[14] The Senate overwhelmingly supported the establishment of the Select Committee, endorsing its creation by a vote of 82-4.[15]

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.[16] The Church Committee subsequently took testimony from hundreds of people, inside and outside of government, in public and private hearings. The NSA, FBI, CIA, IRS, Post Office, and other federal agencies submitted documents. In 1975 and 1976 the Committee issued seven reports and 6 supplemental volumes, classifying another 60 reports for future release.[17]

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.[18] The NSA figured largely in these concerns.

B. NSA Domestic Surveillance

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.[19] Truman's aim was 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.[20] The NSA's mission, accordingly, was to obtain foreign intelligence from foreign electrical communications.[21]

From the beginning, the agency understood foreign intelligence to involve the interception of communications wholly or partly outside the United States and not

---

[13] Interviews with Senator Walter Mondale and Senator Gary Hart, Washington, D.C. (Sept. 23, 2013).
[14] *Id.*
[15] 121 CONG. REC. 1416-34 (1975).
[16] S. Res. 21, 94th Cong. (1975).
[17] Interview with Senator Gary Hart, 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. History Matters, *Rockefeller Commission Report*, *available at* http://history-matters.com/archive/contents/church/contents_church_reports_rockcomm.htm; Press Release, National Security Agency Central Security Service, The National Security Agency Releases Over 50,000 Pages of Declassified Documents (June 8, 2011), http://www.nsa.gov/public_info/press_room/2011/50000_declassified_docs.shtml..
[18] *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. vol. 1-7 (1975).
[19] Presidential Memorandum, Oct. 29, 1952, *amending* National Security Council Intelligence Directive No. 9, Mar. 10, 1950 (National Archives and Records Administration, RG 59, Records of the Department of State, Records of the Executive Secretariat, NSC Files: Lot 66 D 195).
[20] 5 *Intelligence Activities: Hearings on S. Res. 21 Before the Select Comm. to Study Governmental Operations with Respect to Intelligence Activities of the United States*, 94th Cong. 9 (1975) (hereinafter *Church Committee Report, Vol. 5*). 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 (DRAFT REPORT) 1-12, *available at* http://www.maryferrell.org/mffweb/archive/viewer/showDoc.do?docId=145022&relPageId=14.
[21] *Id.* at 6 (statement of General Lew Allen, Jr., Director, National Security Agency).

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."[22]

NSCID 9, however, entitled Communications Intelligence, defined "foreign communications" as "all communications 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."[23] "Foreign communications" thus turned upon the nature of the entity engaged in communications: i.e., a foreign power, or an individual acting on behalf of a foreign power.

The NSA did not (indeed, could not) discuss NSCID 9 during the Church Committee's public hearings. However, the Director of Central Intelligence 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.[24] 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 communication.

Testifying in 1975 before the Church Committee, NSA Director Lieutenant General Lew Allen, Jr. could thus assert that the NSA did not at that time, nor had it (with one exception—i.e., individuals whose names were contained on the NSA's watch list) "conducted intercept operations for the purpose of obtaining the communications of U.S. citizens."[25] Whether such communications were incidentally intercepted, however, was another matter: "some 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."[26]

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 the communications must be outside the country.

Importantly, 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.

---

[22] NSCID 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: Lott 66 D 148, Dulles-Jackson-Correa Report, Annex 12); s*ee also Church Committee Report*, *Vol. 5, supra*, at 6.

[23] NSCID No. 9 (Jul. 1, 1948) (National Archives and Records Administration, RG 59, Records of the Department of State, Records of the Executive Secretariat, NSC Files: Lot 66 D 195); s*ee also* NSCID No. 9, Mar. 10, 1950, *supra*.

[24] *Church Committee Report, Vol. 5*, *supra*, at 9.

[25] *Id.*

[26] *Id.*

1. 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.[27] The program, which operated 1967-1973, 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.[28]

In 1969 the collection of information on individuals included in the watch list became known as Project MINARET.[29] 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].[30]

Senator Mondale asked NSA Director General Lew 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.[31] FISA became the instrument designed to limit the NSA's collection of information on U.S. citizens.

2. 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.[32] The committee decided to discuss the program in open session on the grounds that it was both illegal and violated the Fourth Amendment.[33]

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.[34] For nearly thirty years, the NSA and its

---

[27] *Church Committee Report, Vol. 5, supra*, at 3.
[28] *Id.* at 10-11.
[29] *Id.* at 30.
[30] *Id.* at 36.
[31] *Id.* at 36.
[32] *Church Committee Report, Vol. 5*, *supra*, at 48-57, 60-61, 63; *see also* HOUSE COMM. ON GOV'T OPERATIONS, INTERCEPTION OF INTERNATIONAL TELECOMMUNICATIONS BY THE NATIONAL SECURITY AGENCY (DRAFT REPORT) 2-6, *available at* http://www.maryferrell.org/mffweb/archive/viewer/showDoc.do?docId=145022&relPageId=4 (discussing pressures on the Church Committee from the House side).
[33] *Church Committee Report, Vol. 5*, *supra*, at 57 (statement of Senator Frank Church, Chairman, Select Comm. to Study Governmental Operations with Respect to Intelligence Activities of the United States of the United States Senate).
[34] *Id.* at 57-58.

predecessors received copies of most international telegrams that had originated in, or been forwarded through, the United States.[35]

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.[36]

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.[37] It selected approximately 150,000 messages per month for further analysis, distributing some messages to other agencies.[38]

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 the 20th century problems of intelligence and surveillance."[39] 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.[40]

General Lew 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." Nevertheless, the agency might obtain many unwanted communications; it 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."[41] 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."[42]

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, to allow intelligence agencies to perform their legitimate foreign intelligence activities, without also allowing them to invade U.S. citizens' privacy by allowing them access to information unrelated to national security.[43]

---

[35] *Id*. at 58.
[36] *Id.*
[37] *Id*. at 58-59.
[38] *Id*. at 60.
[39] *Id*. at 65.
[40] *Id.*
[41] *Church Committee Report, Vol. 5*, *supra*, at 19. Former CIA Director William E. Colby provided similar testimony before the Pike Committee 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 Select Committee on Intelligence U.S. House of Representatives*, 94th Cong. 241 (statement of William E. Colby, acting Director of CIA).
[42] *Church Committee Report, Vol. 5*, *supra,* at 20.
[43] *Id.*

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.[44] 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.[45] The Founders' objection to such instruments was simple: were the government to be granted the authority to break into and to search individuals' homes without cause, the private affairs of every person would be subject to inspection.[46] 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.[47]

C. 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 both the exhaustive investigations of Senate Select Committee and other entities stood up to consider the range and extent of programs underway.[48] 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 the refusal to disclose information that might damage national security, in 1971 Senator Ervin called for public hearings to consider "the dangers the Army's program presents to the principles of the Constitution."[49]

In 1975 President Ford issued an executive order establishing the President's Commission on CIA Activities Within the United States ("Rockefeller Commission").[50] Ford appointed Vice President Nelson Rockefeller as Chair.[51] The public charges to which the Rockefeller Commission responded included large-scale domestic surveillance of U.S. citizens; retaining dossiers on U.S. citizens; and aiming such collection efforts at individuals who disagreed with government policies.[52] The Commission's aim was further supplemented by allegations that for the past twenty years the CIA had (a) intercepted and opened personal mail in the United States; (b) infiltrated domestic dissident groups and intervened in domestic politics; (c) engaged in illegal wiretaps and break-ins; and (d) improperly assisted other government agencies.[53]

Like the Senate Select Committee, a key question confronting the Rockefeller Commission was how to define the term "foreign intelligence"—a crucial step in protecting Americans' right to privacy. Accordingly, in its first recommendation, the

---

[44] *Id.* at 71.
[45] *Id.* at 71-72.
[46] *Id.* at 72.
[47] *See, e.g., id.* at 64-65, 84, 125.
[48] *See, e.g., Church Committee Report, Vol. 5, supra,* at 6.
[49] 91 CONG. REC. 26,329.
[50] Exec. Order No. 11,828, 3 C.F.R. 933 (1975).
[51] *Commission on CIA Activities Within the United States: Announcement of Appointment of Chairman and Members*, 11 WEEKLY COMP. PRES. DOC. 25 (Jan. 5, 1975).
[52] REPORT TO THE PRESIDENT BY THE COMMISSION ON CIA ACTIVITIES WITHIN THE UNITED STATES 9 (June 1975).
[53] *Id.*

Rockefeller Commission advised that Section 403 of the 1947 National Security Act be amended to make it explicit that the CIA's activities solely related to "foreign intelligence."[54] Any involvement of U.S. citizens could only be incidental to foreign intelligence collection.[55]

The Commission reinforced the strict separation between foreign targets and U.S. persons through its second recommendation: that the President, via 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." [56]

The House Select Intelligence Committee, in turn, created on February 19, 1975 (known as the Nedzi Committee, after its chair, Lucien Nedzi, Chairman of the Armed Services Committee at the time), was replaced five months later by a committee headed by Representative Otis Pike (D-NY).[57] The Pike Committee focused on a range of intelligence agency intelligence gathering programs—including those of the National Security Agency.[58] Public hearings on the agency's operations were held in October 1975 and February and March 1976.[59] 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.[60]

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 American 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.[61]

For the Pike Committee, these programs violated both Section 605 of the Communications Act and the Fourth Amendment.[62]

The committee expressed particular concern about the NSA's "vacuum cleaner" approach to foreign intelligence gathering.[63] The committee noted that some 24 million telegrams and 50 million telex (teletype) messages entered, left, and transited the United States each year; millions of additional messages traveled over leased lines, "Including millions of computer data transmissions electronically entering and leaving the

---

[54] *Id.* at 12.
[55] *Id.*
[56] *Id.* at 15.
[57] H.R. Res. 138, 94th Cong. (Feb. 19, 1975) (introduced Jan. 16, 1975 and passed Feb. 19, 1975 by a vote of 286-120).
[58] *See, e.g., U.S. Intelligence Agencies and Activities; Intelligence Costs and Fiscal Procedures: Hearings Before the Select Comm. on Intelligence*, 94th Cong. Pt. 1 (1975), printed for the Select Comm. on Intelligence, 58-920 (1975); *U.S. Intelligence Agencies and Activities: Domestic Intelligence Programs: Hearings Before the Select Comm. on Intelligence*, 94th Cong., Pt. 3 (1975), printed for the Select Committee on Intelligence, 53-165 (1976); *U.S. Intelligence Agencies and Activities: Committee Proceedings-Proceedings of the Select Committee on Intelligence*, 94th Cong. Pt. 4 (1975), printed for the Select Comm. on Intelligence, 63-746 (1976).
[59] HOUSE COMM. ON GOV'T OPERATIONS, INTERCEPTION OF INTERNATIONAL TELECOMMUNICATIONS BY THE NATIONAL SECURITY AGENCY (DRAFT REPORT) 2, *available at* http://www.maryferrell.org/mffweb/archive/viewer/showDoc.do?docId=145022&relPageId=4.
[60] *Id.*
[61] *Id.* at 14.
[62] *Id.* at 15-17.
[63] *Id.* at 18.

country"—and international telephone calls presented yet further potential sources of intelligence.[64]

Coming on the heels of the Pentagon Papers (demonstrating 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 President Nixon's resignation on August 9, 1974, the existence of programs investigated by the Church Committee, the Rockefeller Commission, the Pike Committee, and others fed into and deepened the erosion of public confidence in the executive branch. More specifically, their findings undermined citizens' confidence in the intelligence agencies.[65] A critical question facing Congress was 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. 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 engaged in spying on its own citizens.[66]

Justice Powell, writing for the Court, emphasized the limits on the scope 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."[67] Different standards and procedures might apply to domestic security surveillance than those required by Title III of the Omnibus Crime Control and Safe Streets Act of 1968.[68] The Court issued an invitation to Congress to pass new laws covering such cases.[69]

Four critical changes followed. First, consistent with the Church Committee's recommendations, Congress created a permanent Senate Intelligence Committee. Indeed, 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.[70] The new Senate Select Committee on Intelligence ("SSCI") was provided exclusive oversight of the CIA and concurrent jurisdiction over the NSA and other elements of the Intelligence Community ("IC"). The resolution directed that the IC keep the new entity "fully and currently informed" of their activities, including all "significant anticipated activities." 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. The Chair and Vice Chair would not be allowed to serve concurrently as Chair or ranking minority member of any major standing committee.

Of the 15 members selected, no more than 8 would be drawn from the majority party, ensuring balance between the parties. In addition, composition would be built to ensure cross-representation in related committees: two members had to sit each on Appropriations, Armed Services, Foreign Relations, and Judiciary. A limit of eight years

---

[64] *Id.*
[65] 124 CONG. REC. 36,415 (1978).
[66] *United States v. U.S. District Court*, 407 U.S. 297 (1972).
[67] *Id.* at 321-322.
[68] *Id.* at 322.
[69] *Id.* at 323.
[70] S. Res. 400, 94th Cong. (1976).

was placed on committee membership, to avoid intelligence agency capture. Notably, five of the first 15 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—while 14 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.[71]

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."[72]

Executive Order 11905 prohibited the Central Intelligence Agency 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.[73] It prohibited the infiltration of organizations for the purpose of reporting on their activities, unless the organization was primarily composed of Non-US persons and reasonably believed to be acting on behalf of a foreign power.[74] Importantly, the order prevented any *collection* of information about U.S. persons' domestic activities absent situations with clear foreign intelligence or counterintelligence component.[75]

Despite the provisions contained in the Executive Order, Congress considered legislative action to be crucial to reigning in the intelligence agencies. Resultantly, as a third outcome, Congress re-wrote the National Security Act to require a finding and notification for covert action.

Fourth, and most germane to the Judiciary Committee hearing today, 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 simultaneously preventing agencies from using foreign intelligence gathering as an

---

[71] Discussion with William Miller, Washington, D.C. (Sept. 24, 2013). For discussion of the history of the founding of this committee and its subsequent development, *see* LEGISLATIVE OVERSIGHT OF INTELLIGENCE ACTIVITIES: THE U.S. EXPERIENCE, Report, Prepared by the Select Comm. on Intelligence of the United States Senate, 103rd Cong. (1994). *See also* FRANK J. SMIST, CONGRESS OVERSEES THE UNITED STATES INTELLIGENCE COMMUNITY, 1947-1989 (1990); L. BRITT SNIDER, THE AGENCY & THE HILL: CIA'S RELATIONSHIP WITH CONGRESS, 1946-2004, at 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 Intelligence (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 the authorize and appropriate, smaller committees, and the elimination of term limits. U.S. NATIONAL COMMISSION ON TERRORIST ATTACKS UPON THE UNITED STATES, THE 9/11 COMMISSION REPORT: FINAL REPORT 420-21 (2004). (NB: the first proposal to create a joint committee on intelligence was actually made in 1948. *See* H. Con. Res. 186, 80th Cong. (1948) (introduced by Rep. Devitt). 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).

[72] Exec. Order No. 11905, 41 Fed. Reg. 7703 (Feb. 18, 1976). This order was subsequently altered/strengthened by Exec. Order No. 12036, 43 Fed. Reg. 3674 (Jan. 24, 1978) and replaced in part by Exec. Order No. 12333, 46 Fed. Reg. 59941 (Dec. 4, 1981).

[73] Exec. Order No. 11905, § 5(b)(1)-(5), 41 Fed. Reg. 7703 (Feb. 18, 1976).

[74] *Id*. § 5(b)(6).

[75] *Id.* § 5(b)(7).

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 into Congress, and supported by the President and Attorney General, that would require judicial warrants in foreign intelligence cases.[76] Its successor bill, S.1566, became the Foreign Intelligence Surveillance Act of 1978.[77]

III. CONTOURS OF FISA

From the beginning, Congressional members 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.

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 security highlighted the need for this legislation."[78] The debate represented the "final chapter in the ongoing 10-year debate to regulate foreign intelligence electronic surveillance."[79] With the passage of FISA, the Senate would "at long last place foreign intelligence electronic surveillance under the rule of law."[80] 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."[81] Senator Charles Mathais (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."[82]

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 as a foreign power or an agent thereof, *prior to the collection* of the information. 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. For U.S. persons, such probable cause could not be established solely on the basis of otherwise protected First Amendment activities, thus providing American citizens with a higher level of protection. Third, Congress adopted minimization procedures to restrict the type of information that could be obtained and retained. Fourth, FISA made provision for a Foreign Intelligence Surveillance Court ("FISC") to oversee the process. 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.

---

[76] 124 CONG. REC. 35,389 (1978); *see also* Foreign Intelligence Surveillance Act of 1976, S. 3197, 94th Cong (1976).
[77] 124 CONG. REC. 35,389 (1978); *see also* Foreign Intelligence Surveillance Act of 1978, S. 1566, 95th Cong (1978).
[78] 124 CONG. REC. 34,845 (1978).
[79] *Id.*
[80] *Id.*
[81] *Id.*
[82] 124 CONG. REC. 35,389 (1978) (statement of Senator Mathais).

A. Acquisition of Information Tied to Entity Targeted Prior to Collection

From the outset, Congress sought to limit the amount of information acquired by the NSC and others by requiring that the target of surveillance be a foreign power or an agent of a foreign power *prior* to orders being issued to intercept 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 acknowlwedged by a foreign government or governments to be directed and controlled by such foreign government or governments;
(4) a group engaged in international terrorism or activities in preparation therefor;
(5) a foreign-based political organizations, not substantially composed of United States persons; or
(6) an entity that is directed and controlled by a foreign government or governments.[83]

Prior to 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.[84]

Regardless, however, of whether the target was a foreign power (in the strict sense), or a group engaged in international terrorism, in both Houses, throughout the nuanced discussion, underlying the definition of "foreign power" was the understanding that *prior* to collection of information, the government would have to establish that the target—in relation to whom such information would be obtained—qualified as a foreign power or an agent thereof.[85]

In focusing thus on the targets of the communications, Congress rejected the NSA's previous (and now current) reading of what constituted a "target" in relation to data collection.[86] That is, the information to be obtained, *at the moment of acquisition* (not in the context of subsequent analysis—the position advocated by General Allen during the Church Committee hearings and recently resurrected by the NSA), had to relate directly to the individual or entity believed to be a foreign power or an agent thereof.

B. Probable Cause and Satisfaction of Criminal Standards 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". Uppermost in legislators' minds was the need to provide heightened protections for targets of surveillance generally and U.S. citizens in particular. The final bill accomplished this in two ways: adoption of a standard of probable cause and, under certain circumstances, the requirement of a showing of criminal wrongdoing, in order to

---

[83] 50 U.S.C. §1801(a) (2006 & Supp. V 2011).
[84] 124 CONG. REC. 33,782 (1978); *see also* 50 U.S.C. § 1801 (2006 & Supp. V 2011).
[85] 124 CONG. REC. 33,782 (1978).
[86] Testimony of General Lew Allen, Jr., *Church Committee Hearings, Vol. 5, supra,* at 16; Statement of NSA Director Bobby R. Inman, before Senate Subcommittee on Intelligence and Human Rights, as reported in the Washington Post, July 22, 1977, stating "Let there be no doubt, no U.S. citizen is now targeted by the NSA in the United States or abroad."

acquire information. These elements underscore the particularity that Congress insisted upon prior to foreign intelligence gathering.

FISA incorporated a standard of probable cause.[87] Unlike criminal law, however, in which the courts required that probable cause be established that a target had committed, was committing, or was about to commit a particular offense, under FISA, the agency requesting surveillance would have 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.[88]

Under certain circumstances, FISA also required a criminal showing for an entity to be considered a "foreign power". Excluded from this consideration were foreign governments. When they are directly involved, no showing of criminal activity is required. A foreign government, regardless of whether it is an ally or an enemy of the United States, qualifies as a "foreign power."[89]

For groups that qualify as foreign powers because they are engaged in international terrorism, a criminal activity must be involved. 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."[90] Acts in which individuals engage that would qualify them 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 just when it engages in international terrorism, but when engaged in "activities in preparation therefor." This may or may not exceed the criminal "attempt" standard, which is broadly understood as requiring a "substantial step" towards the completion of an offense.[91] Nevertheless, a "group" engaged in preparatory activities for international terrorism would satisfy criminal conspiracy standards.[92]

For agents of a foreign power, Congress inserted heightened protections for U.S. persons.[93] Specifically, FISA defines "agent of a foreign power" as:

---

[87] 50 U.S.C. § 1805(a)(2) (2006 & Supp. V 2011).

[88] *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.") and 50 U.S.C. §1805(a)(3) (2006) (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, for wire and oral communications (e.g., telephone and microphone interceptions), §2516 enumerates predicate offenses that qualify, such as bank fraud (18 U.S.C §1344 (2006)), unlawful possession of a firearm (18 U.S.C. §922(g) (2006)), espionage (e.g., 18 U.S.C. §794 (2006)), assassination (e.g., 18 U.S.C §§351, 1751 (2006 & Supp. V 2011)), sabotage (e.g., 18 U.S.C. §2155 (2006)), and terrorism (e.g., 18 U.S.C. §2332 (2006)). For electronic communications (e.g., e-mail), any federal felony may serve as a predicate. 18 U.S.C. §2516(3) (2006).

[89] 50 U.S.C. §1801(a)(1) (2006 & Supp. V 2011).

[90] 50 U.S.C. §1801(c) (2006 & Supp. V 2011).

[91] *Braxton v. United States*, 500 U.S. 344, 351 (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 (2006). *See also* discussion in *In re [deleted]*, Appendix: Comparison of FISA and Title III.

[92] 18 U.S.C. §371 (2006).

[93] A "United States person" is understood under the statute as "a citizen of the United States, an alien lawfully admitted for permanent resident (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) (2006 & Supp. V 2011).

(1) any person other than a United States person, who –
   (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 frauduluent 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 foreing 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).[94]

What these definitions mean is that U.S. persons may only be considered agents of a foreign power consistent with the five provisions in the second sections. Taken together, three categories emerge for a U.S. person to be considered "an agent of a foreign power": either 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 a par with criminal law must be established prior to 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 with criminal law, specifically with regard to the "may involve" standard of category (a). 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 is involved.

For the second category, sabotage and international terrorism, the term "sabotage" is defined to mean "activities that involve a violation of chapter 105 of Title 18, or that would involve such a violation if committed against the United States."[95] "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

[94] 50 USC §1801(b) (2006 & Supp. V 2011).
[95] 50 U.S.C. §1801(d) (2006 & Supp. V 2011).

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.[96]

These provisions reflect criminal law standards.[97] As the House of Representatives explained at the introduction of 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 and 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."[98]

The third category, which allows a U.S. person to be considered "an agent of a foreign power" for knowingly entering the country under false or fraudulent identity, almost always involves a showing of criminality, for the simple fact that it is not possible to legally enter the United States without providing proof of one's identity to a government official.[99] It is similarly illegal to knowingly assume a false identity on behalf of a foreign power under anti-fraud provisions of the U.S. code.

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 probable cause standard than Title III, those differences are not extensive as applied to U.S. persons.[100]

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

Congress provided yet 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.[101] This was meant to ensure that the executive branch could not place Americans under surveillance simply for exercising their First Amendment rights.

---

[96] 50 U.S.C. §1801(b)(2)(E) (2006 & Supp. V. 2011).
[97] *Compare* 18 U.S.C. §§ 2, 371 (2006) *See also In re [deleted]*, on Appeal from the United States Foreign Intelligence Surveillance Court, Supplemental Brief for the United States, No. 02-001, Appendix: comparison of FISA and Title III, *available at* https://www.fas.org/irp/agency/doj/fisa/092502sup.html.
[98] H.R. Rep. No. 95-1283, Part I, 95th Cong., 2d Sess. 44 (1978).
[99] 18 U.S.C. §1001 (2006).
[100] *In re [deleted],* on Appeal from the United States Foreign Intelligence Surveillance Court, Supplemental Brief for the United States, No. 02-001, Appendix: comparison of FISA and Title III, *available at* https://www.fas.org/irp/agency/doj/fisa/092502sup.html.
[101] 50 U.S.C. §1805(a)(2) (2006).

C. Minimization Procedures for Acquisition and Retention

A third protection inserted by Congress centered on the introduction of minimization procedures, in order to protect activity not related to foreign intelligence from government scrutiny.[102] The legislature insisted here on minimizing not just the analysis of the information, but its "*acquisition* and *retention*."[103] 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 persons. . . [104]

Under FISA, only U.S. persons' information must be subject to minimization procedures.[105]

D. Introduction of the Foreign Intelligence Surveillance Court

As a further precaution against executive overreach, Congress provided in FISA for two courts: the Foreign Intelligence Surveillance Court ("FISC") and the Foreign Intelligence Surveillance Court of Review. 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 this point until the Senate receded and accepted the House language exempting certain particularly sensitive surveillance (i.e., relating solely to foreign powers) from judicial review, 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.[106] 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.[107]

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.[108] Both the FISC judges and the judges on the court of appeal are selected by the Chief Justice of the U.S. Supreme Court.[109] To avoid agency capture, judges may only serve for up to seven years, at the conclusion of which they are not eligible to again serve as FISC judges.[110]

From the beginning, FISC's role was significantly limited: it was merely to grant or to deny applications for orders.[111] The statute thus included extensive details about what would have to be included in such applications: the identity of the Federal officer making the application, 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

---

[102] 50 U.S.C. § 1804(a)(4) (2006 & Supp. V 2011).
[103] 50 U.S.C. § 1801(h) (2006 & Supp. V 2011) (emphasis added).
[104] *Id.*
[105] *Id.*
[106] 124 CONG. REC. 36,409 (1978).
[107] Discussion with former members of the Church Committee, Washington, D.C. (Sept. 23, 2013).
[108] 50 U.S.C. §1803(a)(1) (2006 & Supp. V 2011).
[109] 50 U.S.C. §1803(a)(1) (2006 & Supp. V 2011) and 50 U.S.C. §1803(b) (2006 & Supp. V 2011).
[110] 50 U.S.C. §1803(d) (2006 & Supp. V 2011).
[111] *Id.*

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.[112]

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 only be issued in relation to electronic surveillance. Subsequent amendments expanded FISC's jurisdiction to physical searches, pen registers and trap and trace devices and business records or tangible things.[113] These alterations, however, were merely in substance and not in form. The function being performed by FISC throughout was the same: it was merely to grant or to deny orders prior to the acquisition of information on particular targets.

E. Broad Congressional Support

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. In 1972 the Senate Committee on the Judiciary's Subcommittee on Administrative Practice and Procedure held extensive hearings on the subject of warrantless wiretapping.[114] 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.[115] In 1976 President Ford and Attorney General Levi introduced the first foreign intelligence bill.[116] President Carter and Attorney General Bell subsequently supported S. 1566, which became FISA.[117] Congress consulted the NSA, FBI, CIA, and representatives of interested citizen groups, gaining broad support for the measure.[118]

Because of the bipartisan, multi-branch approach taken to its construction, FISA passed by significant majorities. S. 1566 passed the Senate 95 to 1.[119] H.R. 7308 passed the House 246 to 128.[120] In October 1978 the Senate adopted the Conference Report "by an overwhelming voice vote, with no dissenting voice vote."[121] The House of Representatives, in turn, adopted the Conference Report by a vote of 226 to 176.[122]

F. Subsequent Amendment: Traditional and Non-Traditional FISA

Since FISA's introduction, Congress has amended the statute to cover physical searches,[123] pen register and trap and trace devices,[124] business records,[125] and tangible

---

[112] 50 U.S.C. §1804 (2006 & Supp. V 2011).
[113] 50 U.S.C. §§1821-1824 (2006 & Supp. V 2011) (orders for physical search); 50 U.S.C. §1842 (pen register and trap and trace devices); 50 U.S.C. §1861 (2006) (business records and tangible goods).
[114] 122 CONG. REC. 7543 (1976).
[115] *Id.*
[116] Foreign Intelligence Surveillance Act of 1976, H.R. 12750, 94th Cong. (introduced in the House, Mar. 23, 1976).
[117] 124 CONG. REC. 36,409 (1978).
[118] 124 CONG. REC. 37,738 (1978); 124 CONG. REC. 36,414 (1978).
[119] *Id.*
[120] *Id.*
[121] *Id.*
[122] 124 CONG. REC. 36,417-18 (1978).
[123] Pub L. No. 103-359, §101-909, 108 Stat. 3423, 3443 (1994); 50 U.S.C. §§1821-1829 (2006 & Supp. V 2011).
[124] Pub. L. No. 105-272, §§601-02, 112 Stat. 2396, 2404 (1998); 50 U.S.C. §§1841-1846 (2006 & Supp. V 2011).

goods.[126] Because of their consistent structure and approach, these provisions have come to be referred to collectively as "traditional FISA".[127] In 2008 Congress further amended the statute under Section 702 of the FISA Amendments Act, creating a new, non-traditional surveillance authority. Recent information made public suggests that the NSA is making extensive use of both traditional and modern authorities to conduct broad surveillance programs, in the process obtaining significant amounts of data on U.S. persons. A brief discussion of the provisions helps to underscore Congress' general approach in FISA and to elucidate ways in which these programs violate both the orientation of the statute and the existing statutory language.

1. Traditional FISA: Physical Search, Pen/Trap

Similar to the electronic surveillance provisions, physical search orders under FISA are limited by the government establishing the target of the search prior to acquisition of information. Specifically, physical search orders may only be used to target "premises, information, material, or property used exclusively by, or under the open and exclusive control of, a foreign power or powers."[128] The sub-section 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.[129] It provides for FISC to grant or to deny orders consistent with FISC's role in electronic surveillance.[130] The government must make the same showings, particularly describing the target prior to FISC granting the order.[131] And heightened protections are afforded to U.S. persons.[132]

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).[133] 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

---

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

[126] Various further amendments of these sections have occurred. 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/trap provisions (§214), changed the purpose of electronic & physical searches (§218), and authorized coordination between intelligence and law enforcement (§504). ITRPA subsequently added a "lone wolf" provision via §60001(a).

[127] *See, e.g.,* DAVID S. KRIS AND J. DOUGLAS WILSON, NATIONAL SECURITY INVESTIGATIONS & PROSECUTIONS, Chapter 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 (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) (2006)). 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."

[128] 50 U.S.C. § 1822(a)(1)(A)(i) (2006).

[129] 50 U.S.C. § 1821(1) (2006 & Supp. V 2011).

[130] 50 U.S.C. §§ 1822-1824 (2006).

[131] 50 U.S.C. § 1823 (2006 & Supp. V 2011).

[132] *See, e.g.,* 50 U.S.C. § 1821(1)(A)(ii) (2006 & Supp. V 2011) (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.") and 50 U.S.C. § 1821(1)(A)(iii) (2006 & Supp. V 2011) (requiring minimization procedures for U.S. persons information).

[133] Pub. L. No. 105-272, §§601-02, 112 Stat. 2396, 2404 (1998); 50 U.S.C. §§1841-1846 (2006) (pen/trap); 50 U.S.C. §§1861-1862 (2006) (tangible things).

of the FISA court.[134] 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.[135] 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.[136] Nevertheless, a proper application must be made to the appropriate judicial authority within forty-eight hours.[137]

Following the 9/11 attacks, Congress relaxed the requirement for factual proof for placement of a pen/trap: the applicant no longer must demonstrate why he or she believes that a telephone line will be used by an individual engaged in international terrorism. Instead, the applicant must demonstrate only that the information likely to be gained does not directly concern a U.S. person and will be relevant to protect against international terrorism. This provision, hotly contested by civil libertarians, was scheduled to sunset on December 31, 2005.[138] But in 2006, Congress made it permanent.[139] Critically, while it relaxes the standard for obtaining information from particular telephone lines, it still draws 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—namely: a pen register is:

> [A] device or process which records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facilitiy from which a wire or electronic communication is transmitted, provided, however, that such information shall not include the contents of any communication.[140]

A "trap and trace device", in turn, is defined as:

> [A] device or process which captures the incoming electronic or other impulses which identify the originating number of other dialing, routing, addressing, and signalling 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. [141]

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

(1) the name of the customer or subscriber;
(2) the address of the customer or subscriber
(3) the telephone or instrument number, or other subscriber number of identifier, of the customer or subscriber, including any temporarily assigned network address or associated routing or transmission ifnormation;

---

[134] 50 U.S.C. § 1842(a)-(b) (. 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." 50 U.S.C. § 1842(c)(1)-(2) (2006).

[135] 50 U.S.C. § 1842(c)(A) (2006 & Supp. V 2011).

[136] 50 U.S.C. § 1843(a) (2006 & Supp. V 2011).

[137] 50 U.S.C. § 1843(a)(2) (2006 & Supp. V 2011).

[138] Uniting and Strengthening America by Proving Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act), Pub. L. No. 107-56, § 215, 115 Stat. 272 (2001) (codified as amended at 50 U.S.C. §1861 (2000 & Supp. V 2001)); 18 U.S.C. § 214 (2000).

[139] USA PATRIOT Improvement and Reauthorization Act of 2005, P.L. 109-177, § 102, 120 Stat. 192 (2006).

[140] 18 U.S.C. §3127(3) (2006 & Supp. V 2011).

[141] 18 U.S.C. §3127(4) (2006 & Supp. V 2011).

(4) 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;
(5) 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;
(6) if applicable, any records reflecting period of usage (or sessions) by the customer or subscriber; and
(7) 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.[142]

Notably, what these passages demonstrate is that the collection of all of the information encapsulated in the NSA's telephony metadata program is already provided for under FISA subchapter three.

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.[143] 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.[144] And heightened protections are provided for U.S. persons.[145]

These provisions are entirely consistent with Congress' 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. By inappropriately introducing the telephony metadata under subchapter four, the NSA is simply doing an end-run around the carefully thought-out protections of subchapter three. I will return to this point, below.

2. Traditional FISA: 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.[146] Any records obtained under this provision had to be for "an investigation to gather foreign intelligence information or an investigation concerning international terrorism."[147] 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."[148]

As with the other provisions of traditional FISA, Congress assigned the terms "foreign power", "agent of a foreign power, "foreign intelligence information", and "international terrorism" the same meaning as employed in relation to electronic surveillance.[149] Congress also required intelligence agencies to follow the same steps as

---

[142] 50 U.S.C. §1842(d)(2)(c)(i) (2006 & Supp. V 2011).
[143] 50 U.S.C. §1842(b)(2) (2006 & Supp. V 2011).
[144] 50 U.S.C. §§1842 (d)(2)(A)(i)-(ii) (2006 & Supp. V 2011).
[145] 50 U.S.C. §§1842 (c)(2) (2006 & Supp. V 2011) (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.")
[146] Intelligence Authorization Act for Fiscal Year 1999, Pub. L. 105-272, §602, 112 Stat. 2396, 2410 (1998).
[147] *Id.*
[148] *Id.*
[149] *Id.*

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.[150]

Initially, the FBI did not heavily rely on the business records provision: between 1998 and 2001, the Bureau only used it 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)".[151] Congress eliminated restrictions on the types of businesses or entities on which such an order could be served.[152] 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."[153] Congress again added heightened protections for U.S. persons, requiring that such investigation, where directed towards a U.S. person, not be "conducted solely upon the basis of activities protected by the first amendment to the Constitution."[154]

In the new statute, Congress lowered the standard for obtaining Section 215 orders, eliminating 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.[155]

Nevertheless, from the beginning, the Department of Justice rightly understood that the information to be obtained under the tangible goods provision was still narrow, in that it 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.[156]

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.

---

[150] *Id.*

[151] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism ("USA PATRIOT Act") Act of 2001, Pub. L. 107-56, § 215, 115 Stat. 272, 287 (2001) (codified as amended at 50 U.S.C. § 1861 (2006 & Supp. V 2011). Congress also amended FISA to require that applicants to FISC certify that "a significant purpose" of the surveillance be to obtain foreign intelligence. 50 U.S.C. § 1804(a)(7)(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. *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.

[152] *Id.*

[153] *Id.*

[154] *Id.*

[155] USA PATRIOT Act § 215, Pub. L. 107-56, § 215, 115 Stat. 272, 287 (2001) (codified as amended at 50 U.S.C. § 1861 (2006 & Supp. V 2011).

[156] 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.

For the first two years, attorney general guidelines only allowed business record requests as part of full field investigations. 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 in relation 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."[157] Near future indeed—two days later, on October 31, 2003, Attorney General issued a 38-page document, establishing new guidelines for national security investigations—and allowing agents to obtain business records during preliminary investigations.[158]

Despite the expansion to preliminary investigations, the specificity embedded in the relevance principle remained. In order 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 who may be the target of a recruitment or infiltration effort by an international terrorist, foreign power, or an agent of a foreign power.[159]

There are two points to make about this construction. First, the Attorney General emphasized particular "individuals," "groups," or "organizations" as the target 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).[160] This meant that the target had to be determined (in the course of which the FBI would open a preliminary investigation) prior to orders allowing for the acquisition of tangible goods could issue.

Section 215 of the USA PATRIOT Act was set to expire December 31, 2005.[161] Congress has since renewed it seven times.[162] It is now set to expire June 1, 2015.[163] In

---

[157] *Id.*

[158] The Attorney General's Guidelines for FBI National Security Investigations and Foreign Intelligence Collection (Oct. 31, 2003), *available at* http://www.fas.org/irp/agency/doj/fbi/nsiguidelines.pdf.

[159] *Id.* at 14.

[160] *Id.* at 15.

[161] *Id. See* Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA Patriot Act) of 2001, 50 U.S.C. §§ 1861-63 (amending Title V, Section 501 of the Foreign Intelligence Surveillance Act, "Access to Certain Business Records for Foreign and International Terrorism Investigations, 50 U.S.C. § 1861).

[162] 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); Department of Defense Appropriations Act, 2010, Pub. L. No. 111-118, 123 Stat. 3409 (2009) (allowing for a short-term, 60-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 (2011) (extension until May 27, 2011); PATRIOT Sunsets Extension Act of 2011, Pub. L. No. 112-14, 125 Stat. 216 (2011) (extension until June 1, 2015).

[163] PATRIOT Sunsets Extension Act of 2011, Pub. L. No. 112-14, 125 Stat. 216 (2011). 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, *available at* http://www.washingtonpost.com/politics/patriot-act-extension-signed-into-law-despite-bipartisan-resistance-in-congress/2011/05/27/AGbVlsCH_story.html. A bipartisan group of lawmakers had rallied against the

2005, in the course of extending the tangible goods provision, 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)."[164] The investigation to which the order is tied must be conducted under guidelines approved by the Attorney General.[165] The purpose of the investigation must be "to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities."[166] The underlying investigation may not be directed at a U.S. person based solely on otherwise protected First Amendment activity.[167]

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.[168]

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.[169]

In the 2005 amendments, Congress required "an enumeration of the minimization procedures" related to the retention and dissemination of any tangible things obtained.[170] 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."[171] As discussed, below, the telephony metadata program, by FISC's own admission, fails to satisfy this statutory requirement. 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.[172] Under 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. 1(7) of the U.S. Constitution. See, e.g., *PATRIOT Sunset Extension Act of 2011 "Signed" into Law*, Law Librarian Blog, *available at* http://lawprofessors.typepad.com/law_librarian_blog/2011/05/patriot-sunset-extension-act-of-2011-signed-into-law-.html; 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-auto-pen.html. The White House apparently relied on a memorandum opinion issued by the Office of Legal Counsel in 2005. See Whether the President May Sign a Bill by Directing that His Signature be Affixed to It, Memorandum Opinion for the counsel to the President, July 7, 2005, *available at* http://lawprofessors.typepad.com/files/opinion_07072005.pdf.

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

[165] 50 U.S.C. §1861(a)(2)(A) (2006). Such guidelines are issued consistent with Executive Order 12333.

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

[167] 50 U.S.C. §1861(a)(2)(B) (2006).

[168] 50 U.S.C. §1861(b)(2)(A) (2006) and 50 U.S.C. §1861(c)(1) (2006).

[169] 50 U.S.C. §1861(a)(3) (2006).

[170] *Id.*

[171] 50 U.S.C. §1861(c)(2) (2006).

[172] 50 U.S.C. §1861(c)(2)(E) (2006).

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.[173]

3. Modern FISA and Section 702

Until recently, FISA did not regulate any of the four activities (electronic surveillance, physical searches, pen/trap, or tangible things) when conducted abroad. If a U.S. person went overseas, their telephone calls could be monitored and their hotel room searched without regard to FISA. Authority stemmed from the President's inherent constitutional authority, as channeled through Executive Orders, Department of Defense directives, and policy documents.[174] Nevertheless, in recognition of the higher level of protection afforded to U.S. persons, SIGINT practice, prior to the attacks of September 11, 2001, was not to listen in on, or to collect information on, Americans overseas.[175] U.S. citizens within domestic bounds fell within traditional FISA.

It thus came as a surprise when, in late 2005, the *New York Times* reported that the NSA had "monitored the international telephone calls and international e-mail messages of hundreds, perhaps thousands, of people in the United States without warrants."[176]

White House Press Secretary, Scott McClellan, initially refused to comment.[177] But the next morning, President Bush went on national television to defend the surveillance operation.[178] He grounded his power in the 2001Authorization for the Use of Military Force (passed by Congress one week after the September 11, 2001 attacks), and his

---

[173] 50 U.S.C. §1861(f)(1)(B) (2006).

[174] Exec. Order 12333, § 2.5, 46 Fed. Reg. 59941 (Dec. 4, 1981) "The Attorney General hereby is delegated the power to approve the use for intelligence purposes, within the United States or against a United States person abroad, of any technique for which a warrant would be required if undertaken for law enforcement purposes, provided that such techniques shall not be undertaken unless the Attorney General has determined in each case that there is probable cause to believe that the technique is directed against a foreign power or an agent of a foreign power. Electronic surveillance, as defined in the Foreign Intelligence Surveillance Act of 1978, shall be conducted in accordance with that Act, as well as this order.") *See also* DoD Directive 5240.1, Activities of DoD Intelligence Components that Affect US Persons, Apr. 5, 1988; NSA/CSS Directive No. 10-30, Procedures Governing Activities of NSA/CSS that Affect US Persons, Sept. 20, 1990.

[175] [NSA/Central Security Services] U.S. Signals Intelligence Directive 18 [July 27 1993] at §3.1 ("The policy of the USSS is to TARGET or COLLECT only FOREIGN COMMUNICATIONS.* The USSS will not intentionally COLLECT communications to, from or about U.S. PERSONS or persons or entities in the U.S. except as set forth in this USSID. If the USSS inadvertently COLLECTS such communications, it will process, retain and disseminate them only in accordance with this USSID."). *See also id.* at §4.1.

[176] James Risen and Eric Lichtblau, *Bush Lets U.S. Spy on Callers Without Courts*, N. Y. TIMES, Dec. 16, 2005, *available at* http://www.nytimes.com/2005/12/16/politics/16program.html?pagewanted=all&_r=0 (also writing "Months after the Sept. 11 attacks, President Bush secretly authorized the National Security Agency to eavesdrop on Americans and others inside the United States to search for evidence of terrorist activity without the court-approved warrants ordinarily required for domestic spying. . .")

[177] Press Briefing by Scott McClellan, James S. Brady Briefing Room, 12:33 pm, Dec. 16, 2005, available at http://georgewbush-whitehouse.archives.gov/news/releases/2005/12/20051216-1.html ("there's a reason why we don't get into discussing ongoing intelligence activities, because it could compromise our efforts to prevent attacks from happening. And it could telegraph to the enemy what we are doing. . . And we don't want to do anything to compromise sources and methods. As for talking about the NSA, "that would be getting into talking about ongoing intelligence activities. And they're classified for a reason, because they do to the issue of sources and methods and protecting the American people. And because they're classified, I'm not able to get into discussing those issues from this podium.")

[178] President's Radio Address, Roosevelt Room, Dec. 17, 2005, *available at* http://georgewbush-whitehouse.archives.gov/news/releases/2005/12/20051217.html. ("I authorized the National Security Agency, consistent with U.S. law and the Constitution, to intercept the international communications of people with known links to al Qaeda and related terrorist organizations. Before we intercept these communications, the government must have information that establishes a clear link to these terrorist networks.")

constitutional authorities as Commander-in-Chief.[179] Bush revealed that he had re-authorized the program more than 30 times since 9/11.[180] Each review, he said, had included the Attorney General and the Counsel to the President, with NSA's activities further overseen by legal counsel at DOJ and NSA.[181] Leaders in Congress also had been briefed on the program.[182] Bush added, "This authorization is a vital tool in our war against the terrorists. It is critical to saving American lives."[183] He stated that the release of the *New York Times* story had been illegal.[184] The FBI immediately began an investigation into the leak, with 25 agents and 5 prosecutors assigned to the case.[185]

The Administration soon offered a more detailed legal defense of the Terrorism Surveillance Program ("TSP"), largely consistent with the President's initial statements.[186] The Department of Justice explained that the purpose of the program was to "intercept international communications into and out of the United States of persons linked to al Qaeda or related terrorist organizations".[187] The Department cited "the President's well-recognized inherent constitutional authority as Commander in Chief and sole organ for the Nation in foreign affairs to conduct warrantless surveillance of enemy forces for intelligence purposes."[188] It referenced the President's authority under Article II of the Constitution to repel acts of aggression.[189] And it argued that the language in the AUMF, giving the President to "use all necessary and appropriate force against those nations, organizations, or persons he determines planned, authorized, committed, or aided

---

[179] *Id.* ("I am using authority vested in me by Congress, including the Joint Authorization for Use of Military Force, which passed overwhelmingly in the first week after September the 11th. I'm also using constitutional authority vested in me as Commander-in-Chief.") *See also* Authorization for Use of Military Force, Pub. L. 107-40, 115 Stat 224 (2001).

[180] *Id.*

[181] *Id.*

[182] *Id.*

[183] *Id.*

[184] *Id.*

[185] Scott Shane, Obama Takes a Hard Line Against Leads to Press, N. Y. TIMES, June 11, 2010, *available at* http://www.nytimes.com/2010/06/12/us/politics/12leak.html.

[186] See U.S. Department of Justice, *Legal Authorities Supporting the Activities of the national Security Agency Described by the President* (Jan. 19, 2006) (available at http://www.usdoj.gov/opa/whitepaperonnsalegalauthorities.pdf; Letter from William E. Moschella, Assistant Attorney General to The Hon. Pat Roberts, Chair, Senate Select Committee on Intelligence, The Hon. John D. Rockiefeller, IV, Vice Chairman, Senate Select Committee on Intelligence, The Hon. Peter Hoekstra, Chairman, Permanent Select Committee on Intelligence, U.S. House of Representatives, and the Hon. Jane Harman, Ranking Minority Member, Permanent Select Committee on Intelligence, U.S. House of Representatives, Washington, DC, (Dec. 22, 2005) (available at https://www.fas.org/irp/agency/doj/fisa/doj122205.pdf)

[187] U.S. Department of Justice, *Legal Authorities Supporting the Activities of the national Security Agency Described by the President*, at 5, (Jan. 19, 2006) (available at http://www.usdoj.gov/opa/whitepaperonnsalegalauthorities.pdf)

[188] U.S. Department of Justice, *Legal Authorities Supporting the Activities of the national Security Agency Described by the President*, at 1 (Jan. 19, 2006) (available at http://www.usdoj.gov/opa/whitepaperonnsalegalauthorities.pdf).

[189] U.S. Department of Justice, *Legal Authorities Supporting the Activities of the national Security Agency Described by the President*, at 1 (Jan. 19, 2006) http://www.usdoj.gov/opa/whitepaperonnsalegalauthorities.pdf; and Letter from William E. Moschella, Assistant Attorney General, to The Hon. Pat Roberts, Chair, Senate Select Committee on Intelligence, The Hon. John D. Rockefeller, IV, Vice Chairman, Senate Select Committee on Intelligence, The Hon. Peter Hoekstra, Chairman, Permanent Select Committee on Intelligence, U.S. House of Representatives, and the Hon. Jane Harman, Ranking Minority Member, Permanent Select Committee on Intelligence, U.S. House of Representatives, Washington, DC (Dec. 22, 2005) (available at https://www.fas.org/irp/agency/doj/fisa/doj122205.pdf) ("This constitutional authority," the Assistant Attorney General continued, "includes the authority to order warrantless foreign intelligence surveillance within the United States, as all federal appellate courts, including at least four circuits, to have addressed the issue have concluded.")

the terrorist attacks" of September 11 to prevent "any future acts of international terrorism against the United States" included traditional military activity—into which category warrantless communications intelligence fell.[190] According to DOJ, this moved the decision into the first category of the tripartite framework established by Justice Jackson's concurrence in Youngstown Sheet & Tube Co. v. Sawyer.[191] The government also relied on the War Powers Resolution, enacted less than five years before FISA, as allowing the President to introduce United States Armed Forces into hostilities.[192]

Congress and others strongly objected to the legal analysis. The Authorization of the Use of Military Force nowhere made reference to electronic surveillance; nor did the legislative history associated with the authorization.[193] FISA, moreover, contemplated the advent of war, allowing for special procedures to be followed with respect to electronic surveillance, physical searches and pen/trap surveillance.[194] It provided for a 15 day grace period, to "allow time for consideration of any amendment to [FISA] that may be appropriate during a wartime emergency."[195] At the expiry of the 15 days, absent any amendment, ordinary FISA provisions would have to be followed. This was a carefully-constructed compromise position: during the debates on FISA, the House of Representatives had sought a complete abatement of FISA during periods of declared war. The Senate objected, and the House of Representatives changed its position.

Congress (and the Courts) also had considered and declined to recognize claims to Presidential Article II authority to conduct foreign intelligence gathering within domestic bounds. During passage of FISA, the House wanted the statute to read that it was the "exclusive statutory" means for the Executive to conduct electronic surveillance, implying in the process that the President had inherent surveillance powers outside the statute. The Senate completely rejected this notion, suggesting that if the President were to engage in electronic surveillance outside the parameters of FISA, on judicial review, they wanted the Supreme Court to treat the President's actions as under Justice Jackson's third category in Youngstown: against the expressed intent of Congress. The Senate view carried.

The TSP turned out to be more far-reaching than initially acknowledged. Five months after the initial revelations, on May 11, 2006, a *USA Today* article detailed how, since 9/11, the country's largest telecommunications companies had been secretly providing customers' domestic calling records to the NSA for analysis. AT&T, Verizon, and BellSouth were implicated in the report.[196] Once again, the White House defended the program, stating that no domestic surveillance is conducted without court approval.

---

[190] U.S. Department of Justice, *Legal Authorities Supporting the Activities of the national Security Agency Described by the President*, at 2 (Jan. 19, 2006) (available at http://www.usdoj.gov/opa/whitepaperonnsalegalauthorities.pdf).

[191] U.S. Department of Justice, *Legal Authorities Supporting the Activities of the national Security Agency Described by the President*, at 2 (Jan. 19, 2006) (available at http://www.usdoj.gov/opa/whitepaperonnsalegalauthorities.pdf). *See also Youngstown Sheet & Tube Co. v. Sawyer*, 343 U.S. 579, 635-638 (1952) (Jackson, J., concurring).

[192] U.S. Department of Justice, *Legal Authorities Supporting the Activities of the national Security Agency Described by the President*, at 27 (Jan. 19, 2006) http://www.usdoj.gov/opa/whitepaperonnsalegalauthorities.pdf.

[193] Authorization for the Use of Military Force (AUMF), Pub. L. No. 107-40, § 2(a), 115 Stat. 224 (2001).

[194] 50 U.S.C. §1811 (2006) (electronic surveillance); 50 U.S.C. §1829 (2006) (physical search), 50 U.S.C. §1844 (2006) (pen/trap) ("Notwithstanding any other law, the President, through the Attorney General, may authorize [electronic surveillance, physical search, or pen/trap] to acquire foreign intelligence information for a period not to exceed 15 calendar days following a declaration of war by Congress.")

[195] Foreign Intelligence Surveillance Act of 1978, H.R. Rep. No. 1720, 95th Cong., 2d Sess. at 45 (1978) (Conf. Rep.).

[196] Leslie Cauley, *NSA Has Massive Database of Americans' Phone Calls*, USA TODAY, May 11, 2006, *available at* http://usatoday30.usatoday.com/news/washington/2006-05-10-nsa_x.htm?csp=34.

According to Dana Perino, deputy White House Secretary, the appropriate members of Congress had been briefed.[197] Nevertheless, the news seemed to take the then-Chairman of the Senate Judiciary Committee, Senator Arlen Specter (R-PA) by surprise.[198] Senator Patrick Leahy (D-VT) sounded similarly incredulous, railing against the lack of congressional oversight and suggesting that the media was doing rather a better job of it than the legislature. "Are you telling me that tens of millions of Americans are involved with al Qaeda?" Leahy asked.[199] "These are tens of millions of Americans who are not suspected of anything. . . Where does it stop?"[200] He held up a copy of the newspaper and added, "Shame on us for being so far behind and being so willing to rubber stamp anything this administration does. We ought to fold our tents."[201]

General Michael V. Hayden, NSA director 1999-2005, defended the program to Congress and to the public by saying that the NSA was only targeting international communications – and only those U.S persons suspected of ties to terrorism.[202] According to Hayden, attorneys inside and outside the agency considered that the program was constitutional—and vital to U.S. national security.[203] Hayden's language was strikingly similar to Church Committee hearings and Lt. Gen. Lew Allen Jr.: "This activity was reviewed by proper authority within NSA and by competent external authority. . ."[204] A major difference, of course, was that in the interim Congress had passed FISA, precisely to prevent this type of large-scale collection of information.

In light of growing tension about the program, in 2007 the NSA discontinued it.[205] In April of that year, the Director of National Intelligence J.M. McConnell submitted a proposal to Congress to amend FISA to make it easier for the executive branch to target U.S. interests abroad. Four months later, Congress passed the Protect America Act ("PAA"), easing restrictions on the surveillance of foreigners where one (or both) parties were located overseas.[206] The statute removed FISC from supervising the interception of communications that began or ended in a foreign country. In its place, the Attorney General and the Director of National Intelligence could authorize, up to one year, the acquisition of communications concerning "persons reasonably believed to be outside the United States", where five criteria were met:

1. there were reasonable procedures in place for determining that the acquisition concerns persons reasonably believed to be located outside the United States;
2. the acquisition did not constitute electronic surveillance (meaning it did not

---

[197] *Id.*

[198] *Id.*(reporting Specter as saying that "he would call the phone companies to appear before the panel 'to find out exactly what is going on.'")

[199] *Id.*

[200] *Id.*

[201] *Id.*

[202] *See, e.g.,* Jim Sensenbrenner, Directing the Attorney General to Submit to the House of Representatives all Documents in the Possession of the Attorney General Relating to Warrantless Electronic Surveillance of Telephone Conversations and Electronic Communications of Persons in the United States Conducted by the National Security Agency, H.R. REP. No. 109-382 (2006) (citing, inter alia, Attorney General Alberto Gonzales and General Michael Hayden, Principal Deputy Director for National Intelligence, Press Briefing (Dec. 19, 2005); NSA Director General Hayden Press Conference (Jan. 23, 2006).

[203] *Id.*

[204] *The National Security Agency and Fourth Amendment Rights: Hearings Before the Select Comm. to Study Governmental Operations with Respect to Intelligence Activities of the United States Senate*, 94th Cong. 22 (1976).

[205] S. REP. NO. 110-209, at 4 (2007); and Letter from Attorney General Alberto Gonzales to Senate Judiciary Committee Chairman Patrick Leahy and Senator Arlen Specter (Jan. 17, 2007). Note that these documents suggest that the program ran from just after the attacks of 9/11 until January 2007).

[206] Protect America Act, 2007, Pub. L. 110-55, § 2, 121 Stat. 553. (Aug. 5, 2007) (amending FISA, §105B(a)(1)-(5)), codified at 50 U.S.C. §1805b (2006)).

involve solely domestic communications);

3. the acquisition involved obtaining the communications data from or with the assistance of a communications service provider who had access to communications;
4. a significant purpose of the acquisition was to obtain foreign intelligence information; and
5. minimization procedures outlined in the FISA would be used.[207]

The PAA required the Attorney general to submit the targeting procedures to FISC and to certify that the communications to be intercepted were not purely domestic in nature.[208] Once certified, however, FISC was given no option as to whether or not to grant the order. Twice a year the Attorney General would be required to inform the Intelligence and Judiciary Committees of the House and Senate of incidents or noncompliance with the directive issued by the Attorney General or Director of National Intelligence, incidents of noncompliance with FISC-approved procedures, and the numbers of certifications or directives issued during the reporting period.[209] In addition, the PAA gave retroactive immunity to service providers to insulate them from civil liability. The PAA initially was to operate for six months.[210] Congress then continued it until February 17, 2008.[211] Congress eventually replaced the legislation with a more permanent measure: the FISA Amendments Act ("FAA").[212]

The FAA empowers the Attorney General and the Director of National Intelligence to jointly authorize, for up to one year, "the targeting of persons reasonably believed to be located outside the United States to acquire foreign intelligence information."[213] FISC annually reviews this certification but has no substantive role in the decision either to engage in the surveillance or to cease doing the same. Five limitations apply to the order issued by the AG and DNI: first, it "may not intentionally target any person known at the time of acquisition to be located in the United States."[214] Second, it "may not intentionally target a person reasonably believed to be located outside the United States if the purpose of such acquisition is to target a particular, known person reasonably believed to be in the United States."[215] Third, it "may not intentionally target a United States person reasonably believed to be located outside the United States."[216] Fourth, it "may not intentionally acquire any communication as to which the sender and all intended recipients are known at the time of the acquisition to be located in the United States."[217] And fifth, the collection of such information "shall be conducted in a manner consistent with the fourth amendment to the Constitution of the United States."[218]

---

[207] *Id*.
[208] Protect America Act, 2007, Pub. L. 110-55, § 3, 121 Stat. 552 (Aug. 5, 2007) (amending FISA §105B(c), codified at 50 U.S.C. §1805c (2006).
[209] Protect America Act, 2007, Pub. L. 110-55, §3, 121 Stat. 552 (Aug. 5, 2007) (amending FISA §105C).
[210] Protect America Act, 2007, Pub. L. 110-55, §6 , 121 Stat. 552 (Aug. 5, 2007).
[211] Various bills were proposed in the interim. See, e.g., S. 2248 (2007).
[212] FISA Amendments Act of 2008, Pub. L. 110-261, 122 Stat. 2436 (July 10, 2008).
[213] Foreign Intelligence Surveillance Act, "Procedures for Targeting Certain Persons Outside the United States Other Than United States Persons, Title VII, Section 702, codified at 50 U.S.C. § 1881(a) (2006). Except as otherwise noted, section 702 mirrors the definitions adopted in FISA for the terms "agent of a foreign power", "foreign intelligence information" , "foreign power", and "person".
[214] §1881b(1).
[215] §1881b(2).
[216] §1881b(3).
[217] §1881b(4).
[218] §1881b(5).

The upshot is that Section 702 gives the NSA the authority to target non-U.S. persons located outside the United States at the time of the collection of data.[219] FAA brought the targeting of U.S. persons overseas, previously addressed via Section 2.3 of Executive Order 12333, within traditional FISA. Consistent with the overall approach of FISA, this shift provided a higher protections for U.S. persons. The FAA required, in addition, that the government adopt targeting and minimization procedures for review by FISC. The minimization procedures, in particular, restrict handling information concerning U.S. persons incidentally acquired under Section 702—including the retention and dissemination of such information. In December 2012, Congress passed, and the President signed, the FISA Amendments Act Reauthorization Act, extending Title VII of FISA through December 31, 2017.[220] Absent intervening action by Congress, Title VII will automatically be repealed on that date.[221] Any orders in place as of that date will continue until their ordinary expiration.

IV. NSA TELEPHONY METADATA COLLECTION UNDER §215

On May 24, 2006, the Foreign Intelligence Surveillance Court approved an FBI application for an order, pursuant to 50 U.S.C. §1861, requiring telecommunications providers to turn over all telephony metadata to the National Security Agency.[222] Over the next seven years, FISC issued orders renewing the program thirty-four times.[223] As FISC acknowledged in classified rulings:

> [N]early all of the call detail records collected pertain to communications of non-U.S. persons who are *not* the subject of an FBI investigation to obtain foreign intelligence information, are communications of U.S. persons who are *not* the subject of an FBI investigation to protect against international terrorism or clandestine intelligence activities, and are data that otherwise could not be legally captured in bulk by the government.[224]

This program remained secret until a combination of the Snowden documents and FOIA litigation launched by the Electronic Frontier Foundation forced key documents into the

---

[219] In exigent circumstances, the Attorney General and the DNI may authorize an immediate acquisition under Section 702; however, they must then submit a certification to the FISC as soon as practicable, but in no event later than seven days after they determined the existence of such exigent circumstances.

[220] Foreign Intelligence Surveillance Act (FISA) Amendments Act Reauthorization Act of 2012, Pub. L. No. 112-238, 126 Stat. 1631.

[221] 50 U.S.C.S. §1881 note (LexisNexis Supp. Apr. 2013).

[222] 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-05 (FISA Ct. May 24, 2006), *available at* https://www.eff.org/sites/default/files/filenode/docket_06-05_1dec201_redacted.ex_-_ocr_0.pdf (released by court order as part of the Electronic Frontier Foundation's FOIA litigation). Note that the specific telecommunications company from which such records were sought were redacted, as well as the remaining title; however, the government also released an NSA report that provided more detail on the title of the Order. OFFICE OF THE INSPECTOR GEN., NAT'L SEC. AGENCY/CENT. SEC. SERV., ST-06-0018, REPORT ON THE ASSESSMENT OF MANAGEMENT CONTROLS FOR IMPLEMENTING THE FOREIGN INTELLIGENCE SURVEILLANCE COURT ORDER: TELEPHONY BUSINESS RECORDS (Sept. 5, 2006) (see page 94 of 1846 and 1862 Production, Mar. 5, 2009), *available at* http://www.dni.gov/files/documents/section/pub_Feb%2012%202009%20Memorandum%20of%20US.pdf. For purposes of a more precise citation, I draw from both sources.

[223] 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-paper-section-215.html [hereinafter "Section 215 White Paper"].

[224] In re Production of Tangible Things *From* [REDACTED], Order, 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 (emphasis in original).

public domain.[225] 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.

According to these document, the purpose of the telephony metadata program is to collect information related to counterterrorism and foreign intelligence.[226] The information includes all communications routing information, including (but not limited to) session identifying information (e.g., originating and terminating telephone number, identity of the communications device, etc.), trunk identifier, and time and duration of the call.[227] The metadata collected as part of this program does not include the substantive content of communications [as defined by 18 U.S.C. §2510(8)], nor does it include subscribers' names, addresses, or financial information.[228]

Although many of the details about the telephony metadata program remain cloaked from view, from what has been made public by the government, it appears that the Government takes all information obtained and feeds it into a bulk data set, which is then queried with an "identifier", referred to as a "seed"[229] The NSA uses both international and domestic identifiers.[230]

FISC requires that the NSA establish a "reasonable, articulable suspicion" that a seed identifier used to query the data be 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":

> 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

---

[225] Electronic Frontier Foundation v. U.S. 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 as narrowed by negotiation between the parties in the litigation, 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.").

[226] *See, e.g.*, Section 215 White Paper, *supra* note 223, 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.")

[227] *Id.* at 2.

[228] 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 223, at 3. In addition, the Aug. 9, 2013 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.

[229] Section 215 White Paper, *supra* note 223 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. The Guardian, in turn, reports that the term "identifiers" includes information such as names, telephone numbers, email 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, 12:08 PM), http://www.theguardian.com/world/2013/aug/09/nsa-loophole-warrantless-searches-email-calls (containing screen shot of classified document).

[230] 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.

> 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 "hop" numbers.[231]

It appears that, initially, neither FISC nor the NSA limited the number of "hops" that could be undertaken. It was not until March 2009 that the Government implemented software changes to its system to limit the number of hops permitted to three.[232]

As a practical matter, what this means is that the NSA currently understands the primary order as authorizing the agency to retrieve information as many as three tiers away from the initial identifier.[233] The government refers to this process as "automated chaining."[234] These results can then be further queried "for foreign intelligence purposes."[235] In some cases, this information can then be forwarded to the FBI for further investigation, including using the information thus obtained for applications for an electronic intercept order under Title I of the Foreign Intelligence Surveillance Act.[236]

Like the programs that existed prior to the Church Committee hearings, the range of targets has gradually expanded. Following the initial order, on at least three occasions, the government obtained authorization to expand the telephone identifiers that the NSA could query.[237] And like the programs that led to the creation of FISA in the first place, a significant focus has been on domestic communications.

Since the advent of the program, FISC has understood "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."[238] The government laid out its rationale:

> 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.[239]

The program is thus designed to obtain foreign intelligence or to protect against international terrorist threats in the United States and overseas. Under the statute, the

---

[231] Section 215 White Paper, *supra* note 223, at 3-4.

[232] 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.

[233] Section 215 White Paper, *supra* note 223, at 4.

[234] 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.

[235] Section 215 White Paper, *supra* note 223, at 4.

[236] *Id.*

[237] *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 ("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 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 approved querying related to [REDACTED] Primary Order, docket number BR 08-13, at 8.").

[238] *Id.* at 2 n. 1.

[239] Section 215 White Paper, *supra* note 223, at 3.

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.[240]

Statutory requirements are designed to protect against the collection of information on U.S. persons. Indeed, the statute limits the scope to obtaining foreign intelligence information "not concerning a United States person".[241] Where a U.S. person is involved, it must specifically be "to protect against international terrorism or clandestine intelligence activities."[242]

Despite special protections, the collection of information relating to U.S. persons, who are not themselves the target of any investigation, is central to the program. Indeed, from the beginning, both the government and the Court were fully aware that, as a result of the broad approach—namely, the collection of all information, including that of a purely local nature—such information would be obtained.[243] "Ordinarily," Judge Reggie Walton later wrote, "this alone would provide sufficient grounds for a FISC judge to deny the application."[244] But in the face of Executive Branch claim, under oath, that the program was vital for U.S. national security, the Court acquiesced, requiring only that the Executive follow certain procedural protections.[245] These protections failed to prevent abuses.

The NSA's telephony metadata program contradicts FISA's language, design, and purpose. To understand it otherwise would be to vitiate the statute in terms of Congress' intent in introducing FISA and the general orientation of the statute, as well as the specific statutory restrictions placed on the intelligence agencies and duties assigned to the Foreign Intelligence Surveillance Court. The program also raises constitutional concerns with regard to search and seizure.

V. Bulk Collection Runs Contrary to FISA's General Approach

The telephony metadata program violates the general intent of Congress in enacting FISA—and the approach adopted in the statute itself—in two important ways: first, in its

---

[240] 50 U.S.C. § 1861(b)(2)(A)(i)-(iii) (2006).
[241] § 1861(b)(2)(A).
[242] § 1861(b)(2)(A) (2006 & Supp. V. 2012).
[243] *Id. See* 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 n. 1 (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 ("As the government noted in its application, '[i]f authorized, the requested order will result in the production of call detail records pertaining to [REDACTED] telephone communications, including call detail records pertaining to communications of U.S. persons located within the United States who are not the subject of any FBI investigation.").
[244] In re Prod. of Tangible Things from [REDACTED], Order, 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.
[245] *Id.* (stating that the Court had authorized the bulk collection of call detail records based upon: "(1) the government's explanation, under oath, of how the collection of and access to such data are necessary to analytical methods that are vital to the national security of the United States; and (2) minimization procedures that carefully restrict access to the BR metadata and include specific oversight requirements. Given the Executive Branch's responsibility for and expertise in determining how best to protect our national security, and in light of the scale of this bulk collection program, the Court must rely heavily on the government to monitor this program. . .").

rejection of particularization at the point of acquisition of information; and, second, with regard to the role played by the Foreign Intelligence Surveillance Court.

A. Particularization in Place of Broad Surveillance

The telephony metadata program lacks the particularization that marks Congress' entire approach to domestic foreign intelligence gathering as articulated in the Foreign Intelligence Surveillance Act. Specifically, FISA rejects the wholesale collection of domestic information, insisting instead on minimization; relies on the *prior* targeting of foreign intelligence targets to justify surveillance; provides U.S. persons a heightened level of protection; and 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 at issue in this case. Over the course of Project MINARET, for instance, the watch list expanded to include approximately 1,650 U.S. citizens in total.[246] At no time were there more than 800 U.S. citizens' names on the list, out of a population of about 200 million Americans.[247]

Today, in contrast, there are approximately 316 million Americans, United States Census Bureau, U.S. and World Population Clock (Aug. 28, 2013), http://www.census.gov/popclock/, most of whom would have been subject to the Verizon (and similar) orders issued by the Foreign Intelligence Surveillance Court ("FISC"). This number eclipses the total number of U.S. citizens subject to one of 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 local nature. According to the Director the National Security Agency, Project MINARET did not monitor entirely domestic conversations.[248]

In contrast, the Order issued in April 2013 by FISC specifically *requires* the collection of information "wholly within the United States, including local telephone calls."[249] Set to expire July 19, 2013, the Office of the Director of National Intelligence has confirmed that FISC has again renewed the order.[250]

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

---

[246] *Id.*
[247] *Id.* at 30, 33-34.
[248] *Church Committee Report, Vol. 5, supra*, at 36 (testimony of General Lew Allen, Director, National Security Agency).
[249] 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 (FISA Ct. Apr. 25, 2013).
[250] Press Release, Office of the Dir. of Nat'l Intelligence, Foreign Intelligence Surveillance Court Renews Authority to Collect Telephony Metadata (July 19, 2013), http://www.dni.gov/index.php/newsroom/press-releases/191-press-releases-2013/898-foreign-intelligence-surveillance-court-renews-authority-to-collect-telephony-metadata.

inserted "relevant" into the statute to ensure the continued specificity of targeted investigations.

In addition, Congress empowered the 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 the FISC) that decides which queries to use, and which individuals to target within the database.

This change means that the FISC is not performing its most basic function: protecting U.S. persons from undue incursions into their privacy. Instead, it leaves the determination of whom to target to the agency's discretion. Traditional FISA, as well as authorities under §702, depend upon the criteria in the statute being met *prior to collection of information*. 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 is neither the statutory language nor the government's own internal position. The NSA's own minimization procedures with regard to §702 state:

> In addition to the definitions in sections 101 and 701 of the Act, the following definitions will apply to these procedures:
>
> (a) 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...[251]

2. Prior Targeting to Justify Collection of Data

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."[252] The government sees the enormous number of records as central to the success of the program.[253] Once the records are obtained—i.e., once the "haystack" is created—the government can then go about finding out who the threats are—i.e., the proverbial needles in the haystack.[254]

This process is exactly backwards. The whole point of FISA is for the government to first identify the target, and then to use this 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 runs directly contrary to FISA's design.

3. Heightened Protections for U.S. Persons

In addition, as detailed above, there are myriad ways in which FISA creates extra protections for U.S. persons. The statute itself came from revelations about the rather cavalier manner in which the intelligence agencies were treating Americans' right to

---

[251] 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 (Jan. 8, 2007), *available at* http://epic.org/2013/06/nsa-targeting-and-minimization.html.

[252] Section 215 White Paper, *supra* note 223, at 2.

[253] *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.").

[254] *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) (testimony of Deputy Att'y Gen. James Cole), *available at* http://intelligence.house.gov/video/how-disclosed-nsa-programs-protect-americans-and-why-disclosure-aids-our-adversaries.

privacy. These protections related to the targeting of U.S. persons—not just the later analysis and dissemination of information.

Outside of minimization procedures relating to the downstream manipulation and dissemination of information, the telephony metadata program does not recognize any protection for U.S. persons at the moment of data acquisition. This, too, contradicts the way the statute was structured.

B. Role of the Foreign Intelligence Court

In at least three important ways, the Foreign Intelligence Surveillance Court no longer serves the purpose for which it was designed. First, it was created to determine whether sufficient evidence existed to target individuals within the United States, prior to the collection of such information. But the Court 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 law-making role for the Court. Its decisions were not to serve as precedent, nor was the Court 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, instead of being a neutral, disinterested magistrate, the court has become highly politicized and appears to have failed to act as an effective check on the exercise of surveillance authorities. The manner of appointment of judges to the court, lack of technical expertise, and absence of an effective adversarial process has here harmed the Court's ability to function.

1. Reliance on NSA to Ascertain Reasonable, Articulable Suspicion

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. Documents recently released as a result of court orders in a related FOIA case establish that for nearly three years, the NSA did not follow these procedures[255]—despite the fact that numerous officials at the agency were aware of the violation.[256] Noncompliance incidents have continued. Collectively, these incidents raise serious question as to whether FISC is performing the functions it was designed to address.

a. Failure to Report Initial Noncompliance

---

[255] 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; *see also* 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/.

[256] Declaration of Lieutenant General Keith B. Alexander at 25, 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 (listing seven people in the Signals Intelligence Directive, two from the Office of the General Counsel, and one additional person [REDACTED] 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 email 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 26-27.

Although the NSA had been acting in contravention of 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.[257] 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.[258] The NSA had been using identifiers employed to collect information pursuant to Executive Order 12333—not FISA—to search the telephony database.[259]

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.[260] The Court was not amused.

---

[257] *Id.* at 27

[258] *Id.*

[259] NSA's general SIGINT authorities derive from (1) Exec. Order No. 12333, §1.7, 46 Fed. Reg. 59941 (Dec. 4, 1981) (authorizing the NSA to "Collect (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) Foreign Wireless and Radio Monitoring, National Security Council Intelligence Directive 6 (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 (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. ("[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.

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 AG are located in the Department Defense Regulation 5240.1-R, Procedures Governing the Activities of DOD Intelligence components that Affect United States Persons at 24-37 (Dec. 11, 1982), as well as a classified annex to the regulation overseeing 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.

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. 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 [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 (referring to the first source as the "Address Database" and describing it as "a master target database of foreign and domestic telephone identifiers").

[260] 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*

Judge Reggie Walton expressed concern "about what appears to be a flagrant violation of its Order in this matter."[261] The NSA had repeatedly misled the Court in its handling of the database.[262] FISC immediately issued an order, directing the NSA to undertake a comprehensive review of the NSA's handling of telephony metadata.[263] It gave the government until Feb. 17, 2009 to file a brief to defend its actions and to help the Court to determine whether further action should be taken against the government or its representatives.[264]

The NSA initially admitted only "that NSA's descriptions to the Court 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."[265] It further acknowledged, "the majority of telephone identifiers compared against the incoming BR metadata in the rebuilt alert list were not RAS-approved."[266] 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."[267]

It was not that the NSA was unaware of the requirements established by the statute and by the Court. The Attorney General had, consistent with the primary order, established minimization procedures, amongst 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][3] 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

---

http://www.dni.gov/files/documents/section/pub_Jan%2028%202009%20Order%20Regarding%20Prelim%20Notice%20of%20Compliance.pdf.

[261] *Id.* at 4.

[262] *See, e.g.*, OFFICE OF THE INSPECTOR GEN., NAT'L SEC. AGENCY/CENT. SEC. SERV., ST-06-0018, REPORT ON THE ASSESSMENT OF MANAGEMENT CONTROLS FOR IMPLEMENTING THE FOREIGN INTELLIGENCE SURVEILLANCE COURT ORDER: TELEPHONY BUSINESS RECORDS (Sept. 5, 2006) (see page 94 of 1846 and 1862 Production, Mar. 5, 2009), *available at* http://www.dni.gov/files/documents/section/pub_Feb%2012%202009%20Memorandum%20of%20US.pdf ("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.").

[263] 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.

[264] *Id.* at 2.

[265] Memorandum of the United States In Response to the Court's Order Dated Jan. 28, 2009 at 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.

[266] *Id.* at 11; *see also id.* at 6. Note 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%202%202009%20Order%20from%20FISC.pdf.

[267] 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; *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.

be regarded as associated with [REDACTED] solely on the basis of activities that are protected by the First Amendment to the Constitution.[268]

Nevertheless, apparently, neither the Signals Intelligence Directorate nor the Office of General Council had caught the fact that nearly 90 percent of the queries to the bulk dataset had been illegal.[269] Nor had they realized that their reports to FISC claiming that only RAS-approved numbers were being run against the bulk metadata were false.[270]

In the meantime, the NSA had disseminated 275 reports to the FBI as a result of contact chaining and queries of NSA's archive of telephony metadata.[271] Thirty-one of these had resulted directly from the automated alert process.[272] 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."[273] 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.[274] The government also did not address the dissemination of metadata reports within NSA and subsequent actions taken as a result of the process.

---

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

[269] *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.").

[270] *See, e.g.,* NSA Report to the FISC, Aug. 18, 2006, docket number BR 06-05 (Ex. B to the Government's application in docket number BR 06-08), at 12-15, quoted in Memorandum of the United States In Response to the Court's Order Dated Jan. 28, 2009 at 13, 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 ("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 (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. . .").

[271] Memorandum of the United States In Response to the Court's Order Dated Jan. 28, 2009 at 17, 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; Declaration of Lieutenant General Keith B. Alexander at 42, In re Production 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 (further noting that the 275 reports provided to the FBI tipped a total of 2,549 telephone identifiers as being in contact with identifiers used to query the system).

[272] *Id.*

[273] *Id.* at 17.

[274] *See also* Declaration of Lieutenant General Keith B. Alexander at 36, In re Production 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 ("[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).

Despite the gross violation of FISC's order, the Government argued that FISC should neither rescind nor modify its order.[275] As required by FISC, the NSA had undertaken an end-to-end system engineering and process review (technical and operational) of the NSA's handling of BR 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 BR metadata repository since November 1, 2008 with the purpose of determining if any queries had been made using non-RAS-approved identifiers.[276] The NSA had again trained its employees and adopted new technologies to limit the number of "hops" permitted from an RAS-approved seed identifier to three.[277] 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.[278]

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 §215 of the USA PTRIOT Act.[279] 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.[280] (The NSA had been obtaining 16-digit credit card numbers as well as names/partial names contained in the records of Operator-assisted calls.[281]) It later emerged that an over-collection filter inserted in July 2008 failed to function.[282]

---

[275] 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. 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.

[276] *Id.* at 19.

[277] *Id.* at 20.

[278] *Id.* at 20-21 (listing under "Additional Oversight Mechanisms the government Will Implement": (1) NSA's OGC consulting with 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 SID 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).

[279] *See, e.g.,* Memorandum of the United States In Response to the Court's Order Dated Jan. 28, 2009, In Re Production of Tangible Things From [REDACTED], Docket Number BR 08-13, p. 19, *available at* http://www.dni.gov/files/documents/section/pub_Feb%2012%202009%20Memorandum%20of%20US.pdf (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).

[280] OFFICE OF THE INSPECTOR GEN., NAT'L SEC. AGENCY/CENT. SEC. SERV., ST-06-0018, REPORT ON THE ASSESSMENT OF MANAGEMENT CONTROLS FOR IMPLEMENTING THE FOREIGN INTELLIGENCE SURVEILLANCE COURT ORDER: TELEPHONY BUSINESS RECORDS (Sept. 5, 2006) (see page 95-96 of 1846 and 1862 Production, Mar. 5, 2009), *available at* http://www.dni.gov/files/documents/section/pub_Feb%2012%202009%20Memorandum%20of%20US.pdf ("[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.'").

[281] OFFICE OF THE INSPECTOR GEN., NAT'L SEC. AGENCY/CENT. SEC. SERV., ST-06-0018, REPORT ON THE ASSESSMENT OF MANAGEMENT CONTROLS FOR IMPLEMENTING THE FOREIGN INTELLIGENCE SURVEILLANCE

On October 17, 2008, the government reported to FISC that, after FISC authorized the NSA to increase the number of analysts working with the BR metadata, and had directed that the NSA train the newly-authorized analysts, thirty one (out of 85) analysts subsequently queried the BR metadata in April 2008 *without even being aware that they were doing so*.[283] The upshot was that NSA analysts used 2,373 foreign telephone identifiers to query the BR metadata without first establishing reasonable, articulable suspicion.[284] Despite taking corrective steps, on December 11, 2008, the government notified the Court that an analyst had not installed a modified access tool and, resultantly, had again queried the data using five identifiers for which no reasonable articulable suspicion standard had been satisfied.[285]

Just over a month later, the government informed the Court that, between December 10, 2008 and January 23, 2009, two analysts had used 280 foreign telephone identifiers to query the BR metadata without first establishing RAS.[286]

The process initiated in January 2009 identified additional incidents where the NSA had failed to comply with FISC's orders.[287] In February 2009 the NSA brought two further matters to the court's attention. The first centered on the NSA's use of one of its analytical tools to query the BR metadata, using non-RAS-approved telephone numbers.[288] This tool had been used since the Court's initial Order in May 2006 to search both the BR metadata and other NSA databases.[289] Also in February 2009, the NSA notified NSD that NSA's audit had identified three analysts who conducted chaining the BR metadata using fourteen telephone identifiers that had not been RAS-approved before the queries.[290]

COURT ORDER: TELEPHONY BUSINESS RECORDS (Sept. 5, 2006) (see page 96 of 1846 and 1862 Production, Mar. 5, 2009), *available at* http://www.dni.gov/files/documents/section/pub_Feb%2012%202009%20Memorandum%20of%20US.pdf

[282] In Re Production of Tangible Things from [REDACTED] Order, Docket No. BR 08-13, Mar. 2, 2009, p. 17, *available at* http://www.dni.gov/files/documents/section/pub_March%202%202009%20Order%20from%20FISC.pdf (citing Government's Response to the Court's Order of Jan. 16, 2009, at 13).

[283] Order at 9, In Re Production of Tangible Things from [REDACTED], No. BR 08-13 (FISA Ct. Mar. 2, 2009), *available at* http://www.dni.gov/files/documents/section/pub_March%202%202009%20Order%20from%20FISC.pdf.

[284] *Id.*

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

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

[287] Memorandum of the United States in Response to the Court's Order Dated Jan. 28, 2009 (U), 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; s*ee also* 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/; Section 215 White Paper, *supra* note 223, 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.")

[288] Notice of Compliance Incidents (U) 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.

[289] *Id.* at 3.

[290] 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, United States Army, Director of the National Security

In May 2009, two additional compliance issues arose.[291] The first compliance incident is completely redacted. The second notes a dissemination-related problem: namely, that the unminimized results of some queries of metadata had been "uploaded [by NSA] into a database to which other intelligence agencies. . . had access."[292] According to the government, providing other agencies access to this information may have resulted in the dissemination of U.S. person information in violation of both US Signals Intelligence Directive 18 as well as the more restrictive restrictions imposed by the Court in BR 09-06.[293]

c. FISC Response

Repeatedly, instead of rescinding prior collection programs, FISC merely imposed further requirements on the government.[294] By spring of 2009, the Court had become fed up with the NSA—yet, not 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 NSA return to FISC prior to each query of the database; and that 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: namely, 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. The Court 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 identities], is to obtain and maintain an archive of metadata that will permit these tactics to be uncovered."[295]

According to FISC, the NSA had also suggested that:

Agency 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.

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

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

[293] *Id.*

[294] 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 non-compliance, 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 [FULL LINE 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 (U) at 16, 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.

[295] Order at 2, In Re Production of Tangible Things from [REDACTED], No. BR 08-13 (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%202%202009%20Order%20from%20FISC.pdf.

> "[t]o be able to exploit metadata fully, the data must be collected in bulk. . . The ability to accumulate a metadata archive and set it aside for carefully controlled searches and analysis will substantially increase NSA's ability to detect and identify members of [REDACTED]."[296]

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:

> Access to the archived data shall occur only when NSA has identified a known telephone identifier for which, based on the factual and practical considerations of everyday life on which reasonable and prudent persons act, there are facts giving rise to a reasonable, articulable suspicion that the telephone identifier is associated with [REDACTED].[297]

The Court had a difficult time believing the NSA's claim that its non-compliance with the Court's orders resulted from NSA personnel believing that the Court's restrictions on access to the BR metadata only applied to "archived data" (namely, data located in certain databases). "That interpretation of the Court's Orders," Judge Reggie Walton wrote, "strains credulity."[298] The NSA had compounded its bad behavior by repeatedly submitting inaccurate descriptions of how it developed and used the alert list process.[299] In return for its claim that the program was vital for U.S. national security, the NSA had offered as evidence the rather 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.[300]

FISC objected to the government's assertion that "the Court need not take any further remedial action"[301] Until the NSA completed the review, "the Court sees little reason to believe that the most recent discovery of a systemic, ongoing violation – on February 18, 2009 – will be the last."[302] Accordingly, starting in March 2009, while the NSA could continue to collect data and to test the telephony metadata system, it would only be allowed to query it with a Court order—or, in an emergency, to query the database and then to inform the court by 5:00 pm, Eastern Time, on the next business day.[303] In September 2009, however, FISC lifted the requirement for the NSA to seek approval in every case.

The second protection introduced by FISC was, starting on July 3, 2009, to require the NSA to file a weekly report with the Court, 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 collections with

---

[296] *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 (FISA Ct. Dec. 11, 2008)).
[297] *Id.* at 3 (referencing re-authorization to BR 08-13, dating from Dec. 12, 2008).
[298] *Id.* at 5.
[299] *Id.* at 6.
[300] *Id.* at 13 ("the 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.")
[301] *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)).
[302] *Id.* at 16.
[303] *Id.* at 18–19.

anyone outside NSA." Again, consistent with traditional FISA, the Court 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.[304]

In August 2009 the government submitted its end-to-end assessment of the NSA telephony metadata system.[305] FISC lifted its requirements, leaving dissemination decisions in the future up to the NSA. It is at least questionable the extent to which the requirements with which the NSA was left perform an effective check on the exercise of authorities. Prior to 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."[306] Since 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 as agreed), that the collection of such data is necessary to understand its counterterrorism information, the degree to which this really prevents such dissemination is open to question.

d. Technological Gap

A critical part of FISC's failure to provide effective oversight of the process relates to the Court's decision to have the NSA perform the targeting decision. Part of the problem also stems from the court'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 has an adequate understanding of how the algorithms operate. Neither 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 prior to data mining.

A similar problem may accompany the reporting requirements to Congress. In March 2009, for example, the Department of Justice had 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.[307] A subsequent letter noted that the House and Senate Intelligence and

---

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

[305] 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.

[306] Section 215 White Paper, *supra* note 223, at 5.

[307] Letter from M. Faith Burton, Acting Assistant Attorney General, to the Hon. Patrick J. Leahy, Chairman, Committee on the Judiciary, U.S. Senate; the Hon. Dianne Feinstein, Chairman, Select Committee on Intelligence, U.S. Senate, the Hon. John Conyers, Jr., Chairman, Committee on the Judiciary, U.S. House of Representatives, the Hon. Silvestre Reyes, Chairman, Permanent Select committee 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.

Judiciary Committees had received briefings in March, April, and August, before receiving a copy of the NSA's review in September 2009.[308] To the extent that the representations of the agency are heavily dependent on technical knowledge, the implications may not be readily transparent to lawmaker.

2. Detailed Legal Reasoning and Creation of Precedent

To enforce the specialized probable cause standard encapsulated in the Foreign Intelligence Surveillance Act, Congress created a court of specialized but exclusive jurisdiction.[309] Its job was, narrowly, 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.[310] But even more surprising is the recent public discovery that the Foreign Intelligence Surveillance court has greatly broadened the "special-needs" exception to the Fourth Amendment to embrace wholesale data collection.[311] What is emerging is a complex body of law, establishing doctrines unrecognized by the Supreme Court, which is considered precedent for future applications to FISC.

Specifically, in 2008 FISCR looked back at its decision in *In re Sealed Case* to confirm "the existence of a foreign intelligence exception to the warrant requirement."[312] It acknowledged that FISCR 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."[313]

In *In Re Directives*, FISCR went on to determine that, as a federal appellate court, in the Fourth Amendment context, 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."[314] 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

---

[308] 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/; and Letter from Ronald Weich, Assistant Attorney General, to the Hon. Patrick J. Leahy, Chairman, Committee on the Judiciary, U.S. Senate; the Hon. Dianne Feinstein, Chairman, Select Committee on Intelligence, U.S. Senate, the Hon. John Conyers, Jr., Chairman, Committee on the Judiciary, U.S. House of Representatives, the Hon. Silvestre Reyes, Chairman, Permanent Select committee 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.

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

[310] *Hearing on Strengthening Privacy Rights and National Security: Oversight of FISA Surveillance Program before the S. Judiciary Comm.*, 118th Cong. (July 31, 2013).

[311] *See also* Eric Lichtblau, *In Secret, Court Vastly Broadens Powers of N.S.A.,* NEW YORK TIMES, July 7, 2013, at A1.

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

[313] *Id.*

[314] *Id.* at 1009.

> conclude that this type of foreign intelligence surveillance possesses characteristics that qualify it for such an exception.[315]

The court analogized the exception to the 1989 Supreme Court consideration of the warrantless drug testing of railway workers, on the grounds that a minimal intrusion on privacy could be justified by the government's need to respond to an overriding public danger.[316]

The government subsequently cited *In re Directives* decision in its August 9, 2013 *White Paper*, defending the telephony metadata program, in support of an exception to the Fourth Amendment warrant requirement.[317]

The Foreign Intelligence Surveillance Court continues to go beyond its mandate. In August 2013, for instance, the Court issued a 29-page Amended Memorandum Opinion regarding the July 18, 2013 application by the FBI for the telephony metadata program.[318] Appending the 17-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.[319]

Similarly, in a per curiam opinion of 2002, FISCR suggested "this case raises important questions of statutory interpretation, and constitutionality. After a careful review of the briefs. . . we conclude 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."[320]

Congress did not design the Foreign Intelligence Surveillance Court or the Court of Review to develop its own jurisprudence. Particularly in light of the lack of adversarial process, it is deeply concerning that the Court's decisions have taken on a force of their own. The politicization of the court further underscores the danger inherent in the status quo.

3. Politicization

Congress tried to avoid the politicization of the Foreign Intelligence Surveillance Court by requiring that (a) the eleven 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.[321] To ensure further diversity, any federal district court judge (including a senior judge), who has not previously served on FISC, may be selected.[322] The Foreign Intelligence Surveillance Court of Review, in turn, is comprised of judges selected by the Chief Justice.[323]

The problem with this system is that it has failed. To the extent that political ideology reflects in the appointments process, the court can only be viewed as highly politicized. The past two Chief Justices have been appointed by Republican presidents, and their selections for the Foreign Intelligence Surveillance Court and Court of Review have been heavily weighted towards judges that have been nominated by Republican Administrations. (See *Fig. 1*) Only one of the current eleven judges serving on FISC is a

---

[315] *Id.* at 1011.
[316] Skinner v. Ry. Labor Execs. Ass'n, 489 U.S. 602, 620 (1989).
[317] Section 215 White Paper, *supra* note 223, at 15.
[318] In Re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible things from [REDACTED], No. BR 13-109 (FISC. 2013).
[319] *Id.*
[320] In Re Sealed Case No. 02-002, (FISA Ct. of Rev., Sept. 9, 2002).
[321] 50 U.S.C. §1803(e), (d) (2010).
[322] 50 U.S.C. §1803(a) (2010).
[323] 50 U.S.C. §1803(b) (2010).

Democratic nominee. Over the past decade, of the 20 judges appointed to FISC and FISCR, only three were democratic nominees to the bench.

At least two of the nominees to the court over the past decade, moreover, have rejected FISA as being an unconstitutional intrusion on the President's inherent authorities. Laurence Silberman, from the DC Circuit, testified to Congress in 1978 (when FISA was being debated) that the legislation violated the U.S. Constitution.[324] 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."[325] For Silberman, the judiciary's role in any national security electronic surveillance should be circumscribed. He explained,

> 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.[326]

The chief concern was not a so-called "imperial Presidency", but the advent of an imperial judiciary. The authorities thus transferred to the Foreign Intelligence Surveillance Court represented an unconstitutional erosion of executive power.[327] In addition to Silberman, Ralph Guy, a 6th Circuit judge, as a U.S. attorney, argued for the government in *U.S. v. U.S. District Court*, that the president did not need any type of a warrant to engage in national security surveillance.[328]

Along with Judge Leavy, a Reagan appointee, 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 where the primary purpose of the investigation was criminal in nature.[329]

The FISCR panel that created a foreign intelligence exception to the Fourth Amendment warrant requirement similarly lacked a diverse political base: the three-judge panel included Chief Judge Selya and Senior Circuit Judges Winter and Arnold—the first two appointees of Ronald Reagan and the last of George H.W. Bush.

JUDGES APPOINTED TO THE FOREIGN INTELLIGENCE SURVEILLANCE COURT AND COURT OF REVIEW BY ORIGINAL APPOINTMENT TO THE BENCH[330]

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

[324] *Foreign Intelligence Electronic Surveillance: Hearings on H.R. 5794, 9745, 7308, and 5632 Before the Subcomm. on Legislation of the Permanent Select Comm. on Intelligence*, 95th Cong., 2d Sess. 221 (1978) (statement of Laurence H. Silberman, Feb. 8, 1978).
[325] *Id.*
[326] *Id.* at 219.
[327] *Id.*
[328] *United States v. U.S. Dist. Ct. for the E. Dist. of Mich.*, 407 U.S. 297 (1972).
[329] *In re Sealed Case* No. 02-002, Foreign Intelligence Surveillance Court of Review, Sept. 9, 2002.
[330] Dates of appointment obtained from the Federation of American Scientists, available at http://www.fas.org/.

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 Webber Wright*	FISC	5/19/2009 – 5/18/2016	George H.W. Bush
Thomas Hogan*	FISC	5/19/2009 – 5/18/2016	Ronald Reagan
Morris Arnold**	FISCR	6/13/2008 – 5/18/2015	George H.W. Bush
James 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 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 Edward Conway	FISC	5/19/2002 – 10/30/2003	Ronald Reagan
Edward Leavy	FISCR	9/25/2005 – 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 Stafford	FISC	5/19/1996 – 5/18/2003	Gerald Ford
Royce C. Lamberth	FISC	5/19/1995 – 5/18/2002	Ronald Reagan
Laurence Silberman	FISCR	6/18/1996 – 5/18/2003	George W. Bush
Paul Roney	FISCR	9/13/1994 – 05/18/2001	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 Ray Baldock	FISCR	6/17/1992 – 5/18/1998	Ronald Reagan
Ralph G. Thompson	FISC	6/11/1990 – 5/18/1997	Gerald Ford
Frank Freedman	FISC	5/30/1990 – 5/19/1994	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 Seitz	FISCR	3/19/1987 – 3/18/1994	Lyndon B. Johnson

** Denotes current members of FISC* *Figure 1*

***Denotes current members of FISCR*

Augmenting the politicization of FISC and FISCR is the rather remarkable success rate enjoyed by the government in its applications to the court. Scholars have noted that it is "unparalleled in any other American court."[331] Much attention has been paid in this regard to the almost nonexistent rate of denial of orders under the electronic communications intercept authorities. Almost no attention, however, has been paid to business records and the production of tangible goods under 50 U.S.C. §1862(c)(2)—the section most relevant to the metadata programs. Consistent with the restrictions, 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. (See *Fig. 2*)

ORDERS FOR THE PRODUCTION OF TANGIBLE GOODS

Year	Number of Applications to FISC under 50 USC 1862(c)(2)	Number of Applications Granted by FISC
2005[332]	155	155
2006[333]	43	43
2007[334]	6	6
2008[335]	13	13
2009[336]	21	21
2010[337]	96	96
2011[338]	205	205
2012[339]	212	212

Figure 2

These numbers are remarkable not least because any one order, as we have seen with the telephony metadata program, could result in the collection of millions of records on millions of U.S. persons. In light of the utter lack of adversarial counsel in in camera, ex parte proceedings, these numbers at least raise serious question about the extent to which FISC and FISCR perform the function they were envisioned to serve.

---

[331] Ruger, *supra* note 309, at 245.

[332] Letter from William E. Moschella, Assistant Attorney General, to the Hon. Richard B. Cheney, President, United States Senate, Apr. 28, 2006, *available at* http://www.justice.gov/nsd/foia/foia_library/2005fisa-ltr.pdf.

[333] Letter from Richard A. Hertling, Acting Assistant Attorney General, to the Hon. Richard B. Cheney, President, United States Senate, Apr. 27, 2007, *available at* http://www.justice.gov/nsd/foia/foia_library/2006fisa-ltr.pdf.

[334] Letter from Brian A. Benczkowski, Principal Deputy Assistant Attorney General, to the Hon. Richard B. Cheney, Apr. 30, 2008, *available at* http://www.justice.gov/nsd/foia/foia_library/2007fisa-ltr.pdf.

[335] Letter from Ronald Weich, Assistant Attorney General, to the Hon. Joseph R. Biden, Jr., President, United States Senate, May 14, 2009, *available at* http://www.justice.gov/nsd/foia/foia_library/2008fisa-ltr.pdf.

[336] *Letter from Ronald Weich, Assistant Attorney General to the Hon. Joseph R. Biden, Jr., President, United States Senate, Apr. 30, 2010, available at http://www.justice.gov/nsd/foia/foia_library/2009fisa-ltr.pdf.*

[337] Letter from Ronald Weich, Assistant Attorney General to the Hon. Joseph R. Biden, Jr., President, United States Senate, Apr. 29, 2011, *available at* http://www.justice.gov/nsd/foia/foia_library/2010fisa-ltr.pdf.

[338] Letter from Ronald Weich, Assistant Attorney General to the Hon. Joseph R. Biden, Jr., President, United States Senate, Apr. 30, 2012, *available at* http://www.justice.gov/nsd/foia/foia_library/2011fisa-ltr.pdf.

[339] Letter from Peter J. Kadzik, Principal Deputy Assistant Attorney General, to the Hon. Joseph R. Biden, Jr., President, United States Senate, Apr. 30, 2013, *available at* http://www.justice.gov/nsd/foia/foia_library/2012fisa-ltr.pdf.

VI. BULK COLLECTION VIOLATES FISA'S STATUTORY PROVISIONS

The telephony metadata program violates the express statutory language in three primary areas: first, with regard to the language "relevant to an authorized investigation"; second, in relation to the requirement that the information sought can be obtained 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 local nature, are "relevant" to foreign intelligence investigations.

The word itself, the administration states, "is a broad term that connotes anything '[b]earing upon, connected with, [or] pertinent to' a specified subject matter. 13 Oxford English Dictionary 561 (2d ed. 1989)."[340] Turning to its "particularized legal meaning,"

> It is well-settled in the context of other forms of legal process for the production of documents that a documents 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.[341]

The fact 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.[342]

Applied to the telephony metadata program, whilst 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."[343] For communications data, the government argues, connections between individual data points can only be reliably identified through large-scale data mining.[344]

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 to authorized investigations; the center revolves around the connection in the statutory language between the relevance of the information to be obtained and "an authorized investigation."

1. Relevance Standard

The first problem with the government's argument is that it stretches credulity to state that there are "reasonable grounds" to believe that millions of daily telephone records are "relevant" to an authorized investigation.

The records sought by the government under the telephony metadata program detail the interactions, personal and business relationships, religious and political connections,

---

[340] Section 215 White Paper, *supra* note 223, at 8.
[341] *Id.* at 9.
[342] *Id.* at 2–3.
[343] *Id.* at 3.
[344] *Id*.

and other intimate details – on a daily basis – of millions of Americans, not themselves connected in any way to foreign powers 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. Rape hotlines, abortion clinics, and political party headquarters—all telephony metadata data is being collected by the NSA.

Reading FISA to allow this type of collection would render meaningless the qualifying phrases contained in 50 U.S.C. §1861(b)(2)(A). The statute first requires that there be "reasonable grounds" to believe that the records being sought are relevant. Although FISA does not define "reasonable grounds", it has been treated as the equivalent of "reasonable suspicion".[345] This standard requires a showing of "specific and articulable facts, which, taken together with rational inferences from those facts, reasonably warrant" an intrusion into an individual's right to privacy.[346]

The FISC order requires that Verizon disclose all domestic telephone records—including those of a purely local nature. According to Verizon Communications News Center, as of last year, the company has 107.7 million wireless customers, connecting an average of 1 billion calls per day.[347] There is simply no way that the government provided specific and articulable facts relevant to each one of those customers or calls, sufficient to establish reasonable grounds to establish their relevance. Interpreting relevance as including all records is so broad as to make the "reasonable grounds" requirement obsolete.

Precisely what, in turn, makes a tangible good "relevant" to an authorized investigation is not explained in the statute. Nevertheless, the act suggests that tangible things are "presumptively relevant where they: "pertain 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.[348]

This section also 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 millions simply pushes the bounds of common sense. So the telephony metadata is neither relevant nor presumptively relevant.

The government's interpretation is so broad that it establishes a dangerous precedent. If all telephony metadata is relevant to foreign intelligence investigations, then so is all email metadata, and all GPS metadata, all financial information, all banking records, all social network participation, and all Internet use. Indeed, FISC has hinted that there may be other programs at there that operate in a similar fashion, and on September 28, 2013, the *New York Times* reported that the NSA began allowing analysis of phone call and email logs in November 2010 to begin examining American's networks of

---

[345] *See, e.g.*, United States v. Banks, 540 U.S. 31, 36 (2003); United States v. Henley, 469 U.S. 221, 227 (1985); United States v. Brinoni-Ponce, 422 U.S. 873, 881–82 (1975); Kris & Wilson, *supra* note 127, at §19:3.

[346] Terry v. Ohio, 392 U.S. 1, 21 (1968).

[347] Verizon Communications Company Statistics, reported by Verizon Communications News Center, Aug. 10, 2012, *available at* http://www.statisticbrain.com/verizon-communications-company-statistics/.

[348] 50 U.S.C. §1861(b)(2)(A) (2006).

associations.[349] If all telephony metadata is relevant, then so is 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 FISA in the first place.

Finally, the government's interpretation directly contradicts Congress' intent in adopting §215. At the introduction of the measure Senator Arlen Specter explained that the purpose of the language was 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.[350] During a House Judiciary Committee meeting on July 17, 2013, Representative James Sensenbrenner (R-WI), reiterated that the reason Congress inserted "relevant" into the statute was 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.[351] Members of the Committee made similar claims.[352]

2. Connection to "an Authorized Investigation"

There are three ways, in turn, in which the telephony metadata program violates FISA's requirement in §1861 that the order be sought for use in an "authorized investigation." First, the guidelines establishing when such an investigation exists relate solely to the moment of the *collection* of the information. The FISC order, in 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 *prior* to the collection of information—namely, that the investigation be premised upon specific individuals, groups, or organizations, or violations of criminal law. The telephony metadata program, in contrast, requires no such specificity prior to 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 relevant to the concept of investigations generally. This means that the orders do not, in fact, relate to (existing) authorized investigations.

a. Collection of the Information

FISA, as aforementioned, 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).[353] It ties the definition of what constitutes an authorized investigation to guidelines approved by the Attorney General under Executive Order 12333.[354] These guidelines establish three levels of investigative activity in national security investigations: (1) threat assessments, (2) preliminary investigations, and (3) full investigations.[355]

FISA makes it clear that the tangible records in question may *not* be sought as part of the first level of national security investigations—i.e., the threat assessment stage. There

---

[349] James Risen and Laura Poitras, *NSA Gathers Data on Social Connections of U.S. Citizens*, NEW YORK TIMES, Sept. 28, 2013, at A1.
[350] 151 Cong. Rec. 13,441 (2005).
[351] *Oversight of the Administration's Use of FISA Authorities: Hearing Before H. Comm. on the Judiciary*, 113th Cong. (2013).
[352] *Id.*
[353] 50 U.S.C. §1861(b)(2)(A) (2006).
[354] *Id.*
[355] The Attorney General's Guidelines for FBI National Security Investigations and Foreign Intelligence Collection at 3 (Oct. 31, 2003), *available at* http://www.fas.org/irp/agency/doj/fbi/nsiguidelines.pdf [Redacted in part] [hereinafter AG NSI Guidelines]

is an important reason for this restriction: threat assessment is the most general level of an investigation. It allows the FBI to 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."[356] To protect individual rights, the only types of methods allowed, as noted by the Attorney General, are "relatively non-intrusive investigative techniques." This includes:

> obtaining 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-pretextual interviews and requests for information from members of the public and private entities, and accepting information voluntarily provided by governmental or private entities.[357]

Nowhere in the discussion of the threat assessment stage does the document contemplate the use of court-ordered surveillance.

The guidelines go on to compare the authorization of the first level of investigations to authorization under Part VI of the Attorney General's Guidelines on General Crimes. These guidelines state that mail covers, mail openings, and nonconsensual electronic surveillance or any other investigative technique covered by Title 18 U.S.C. §§2510-2521 *shall not be used during a preliminary inquiry*.[358]

The point of these limits is to place a higher burden on the government to justify the use of more intrusive surveillance. That is, if such information is going to be *collected*, there must be a higher burden of proof on the government to justify the *collection* of data. It is for this reason that what distinguishes the first level of threat assessment from the second level "preliminary investigation" is the type of information that can be *obtained*. It is thus the act of collecting it that characterizes the distinction between the different levels

In contrast to the guidelines, the primary order authorizing the telephony metadata program authorizes the *collection* of data for 90-day periods, in the course of which the NSA may *search* the information in connection with an authorized investigation.

The primary order is general—it states that there are reasonable grounds to believe not that the information is relevant to a particular investigation, but rather, in the plural, to "authorized investigations".[359] The idea is that the general collection of records may be relevant to any number of investigations. This is precisely the government's argument in its August 2013 white paper: "there have been numerous FBI investigations in the last several years to which the telephony metadata records are relevant."[360] Under the guidelines, it is the *collection* of such information that is premised upon the existence of an authorized investigation—not the *search* of broad data in the course of the same.

b. Specificity

For both preliminary investigations and full investigations, for which tangible items orders under FISA may be sought, there is a predicate specificity required *prior* to the collection of information—namely, that the investigation be premised upon specific

---

[356] *Id.* at 3.
[357] *Id.* at 3.
[358] Attorney General's Guidelines on General Crimes, Racketeering Enterprise and Domestic Security/Terrorism Investigations II(b)(5)(a)-(c), *available at* http://www.justice.gov/ag/readingroom/generalcrimea.htm#general.
[359] *See* Primary Order at 2, In Re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things From [REDACTED], No. BR 13-80 (FISA Ct. Apr. 25, 2013), *available at* http://www.dni.gov/files/documents/PrimaryOrder_Collection_215.pdf.
[360] Section 215 White Paper, *supra* note 223, at 6.

individuals, groups, or organizations, or violations of criminal law. The telephony metadata program, in contrast, collects all call records.

Under the Attorney General guidelines, preliminary investigations are authorized "when there is information or an allegation indicating that a threat to the national security may exist."[361] Such investigations are particular, in that they may relate to specific individuals, groups, and organizations.[362] The guidelines state,

> Since the legal predicate for mail opening, physical searches, and electronic surveillance that require a judicial order or warrant generally entails more substantial information or evidence than would be available outside of a full investigation, the Guidelines specify that these methods are *not* available in preliminary investigations.[363]

Pen registers and trap and trace devices may be used during preliminary investigations.[364] Such investigations are limited: they are initially authorized for up to six months, subject to a possible six-month extension. Extensions beyond a year must be authorized by FBI Headquarters.[365]

Full investigations, in turn, require specific and articulable facts giving reason to believe that a threat to national security may exist.[366] Like preliminary investigations, such inquiries as specific in that they may relate to individuals, groups, and organizations.[367]

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, outside of their actual scope.

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 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."[368] The word "are" before "relevant" suggests that at the time the records are being sought, their relevance to an investigation must be established.

The orders issued by FISC depart from the statutory language, empowering the NSA to obtain the data in light of their relevance to "authorized investigations"—and requiring telecommunications companies to indefinitely provide such information in the future.[369] But how can the court know that all such telephony data will continue to be relevant to investigations that are not yet opened? Indeed, as noted by amici in *In Re Electronic Privacy Information 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.

---

[361] AG NSI Guidelines, p. 3.
[362] *Id.* at 4.
[363] *Id.* (emphasis added).
[364] *Id.*
[365] *Id.*
[366] *Id.*
[367] *Id.*
[368] 50 U.S.C. §1861(b)(2)(A) (2006).
[369] Primary Order at 2, In Re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things From [REDACTED], No. BR 13-80 (FISA Ct. Apr. 25, 2013), *available at* http://www.dni.gov/files/documents/PrimaryOrder_Collection_215.pdf ("[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. . .")

Instead, Congress required relevance to an investigation existing at the time of the application."[370]

In addition, the information sought must be relevant "to an authorized investigation." This is both singular ("an") and past tense, in that is 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*."[371] 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. Namely, 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."[372] That is, it is the nature of the information extracted, not the prior existence of a directly related, authorized investigation, that is of moment. Authorized investigations thus become merely a category for which the information is useful.[373]

This interpretation directly contradicts Congressional intent. Following the release of the Snowden documents, Representative F. James Sensenbrenner, one of the principal authors of the USA PATRIOT Act, noted that in Section 215, "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."[374]

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."[375] FISC, accordingly, took the position in its order authorizing the telephony metadata program that "The tangible things sought could 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."[376] The court later explained, "Call detail records satisfy this requirement, since they may be obtained by (among other means) a 'court order for disclosure' under 18 U.S.C.A. §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."[377]

---

[370] Brief for Cato Institute as Amicus Curiae Supporting Petitioner, In Re Electronic Privacy Information Center, No. BR 13-80 (FISA Ct. Apr. 25, 2013) (No. 13-58), at *4.
[371] H.R. REP. NO. 107-236, at 61 (2001) (emphasis in original).
[372] Section 215 White Paper, *supra* note 223, at 8–9.
[373] See *id.* at 6 ("The telephony metadata records are sought for properly predicated FBI investigations into specific international terrorist organizations and suspected terrorists.")
[374] Rep. Jim Sensenbrenner, This Abuse of the Patriot Act Must End, The Guardian (U.K.), June 9, 2013, http://www.theguardian.com/commentisfree/2013/jun/09/abuse-patriot-act-must-end.
[375] 50 U.S.C. §1861(c)(2)(D) (2006).
[376] *Id.* at 3.
[377] Supp. Op. at note 1, In Re Production of Tangible Things from [REDACTED], No. BR 08-13, (FISA Ct. [date]) (emphasis in original).

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, &c., over which he has control and which help to elucidate the matter in issue.[378] Unlike warrants, something less than probable cause is required. 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.[379]

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."[380] Precisely what counts as reasonable (or not) is heavily context-dependent.[381] In *United States v. Nixon*, 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.[382]

The *Nixon* standard does not apply in the context of grand jury proceedings.[383] In 1991 the Court explained:

> *Nixon's* multi-factor test would invite impermissible procedural delays and detours while courts evaluate the relevance and admissibility of documents sought by a particular subpoena. Additionally, 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.[384]

The Court went on to note that this does not mean that the grand jury's investigatory powers are limitless. To the contrary, it is still subject to Rule 17(c). Nevertheless, grand jury subpoenas are given the benefit of the doubt, with the burden of showing unreasonableness on the recipient seeking to avoid compliance.[385] 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."[386]

At the broadest level, then, FISC's assertion, at least with regard to a grand jury subpoena, appears to be valid. But there are three critical flaws in the court'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 openly 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.

1. Not for Fishing Expeditions

Even with such deference granted to subpoenas issued by grand juries, such instruments may *not* be used for fishing expeditions—i.e., enabling individuals to obtain massive

---

[378] 3 WILLIAM BLACKSTONE. COMMENTARIES *382.
[379] Joshua Gruenspecht, *"Reasonable" Grand Jury Subpoenas: Asking for Information in the Age of Big Data*, 24 HARV. J. OF L. & TECH. 544 (2011).
[380] Fed. R. Crim. P. 17C.
[381] New Jersey v. T.L.O., 469 U.S. 325, 337 (1985).
[382] United States v. Nixon, 418 U.S. 683, at 699-700 (1974).
[383] United States v. R. Enterprises, Inc., 498 U.S. 292 (1991).
[384] *Id.* at 292-93.
[385] *Id.* at 293.
[386] *Id.*

amounts of information whence evidence can be derived.[387] That is to say, a grand jury 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, in order for the Court to order its production. A general suspicion that collecting and analyzing all telephone records in the United States might yield some evidence of criminality is many steps removed from the prior suspicion of a particular act of criminality that characterizes grand jury subpoenas.

Almost all of the telephony metadata collected is utterly unrelated to criminal activity. In Judge Reggie Walton's words,

> [N]early all of the call detail records collected pertain to communications of non-U.S. persons who are not the subject of an FBI investigation to obtain foreign intelligence information, are communications of U.S. persons who are not the subject of an FBI investigation to protect against international terrorism or clandestine intelligence activities, and are data that otherwise could not be legally captured in bulk by the government. Ordinarily, this alone would provide sufficient grounds for a FISC judge to deny the application.[388]

Precisely because the information is not connected, in any way, to criminal activity, Walton suggests that it could not, in any other way, even be collected.

While new technologies may change what is possible in terms of the amount of records obtained or the level of insight that can be gleaned, they do not invalidate the underlying principle. In a world limited by the physical manifestation of evidence, practicality helped to cabin the scope of subpoenas. Digitization, however, does not alter the importance of tying the compulsion of evidence directly to an underlying crime.

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.

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 would 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, the "vast majority" of which (according to FISC's own language) are of a purely local nature, are swept up by the NSA.[389]

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. Most of the individuals in the database are suspected of no wrongdoing whatsoever. Yet the minimization

---

[387] *Id.* at 299 ("Grand juries are not licensed to engage in arbitrary fishing expeditions.").
[388] FISC Order, Mar. 5, 2009, p. 12, *available at* http://www.dni.gov/files/documents/section/pub_March%202%202009%20Order%20from%20FISC.pdf. Order at 9, In Re Production of Tangible Things from [REDACTED], No. BR 08-13 (FISA Ct. Mar. 2, 2009), *available at* http://www.dni.gov/files/documents/section/pub_March%202%202009%20Order%20from%20FISC.pdf.
[389] FISC Order at 2, No. 06-05 (FISA Ct. May 24, 2006), *available at* http://s3.documentcloud.org/documents/785206/pub-may-24-2006-order-from-fisc.pdf.

procedures allow for any information obtained from mining the data to then be used in criminal prosecution. This is an unprecedented use of subpoena information-gathering authority. It amounts 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.[390]

Later in the document, he again noted that the information "otherwise could not be legally captured in bulk by the government".[391]

This assertion directly contradicts the statutory requirement that the information could otherwise be obtained via subpoena duces tecum. It amounts to an admission, by the Court, that the program violated the statute.

What makes the failure of the Court to prevent the illegal program from continuing 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 continues,

> Nevertheless, the FISC has authorized the bulk collection of call detail records in this case based upon: (1) the government's explanation, under oath, of how the collection of and access to such data are necessary to analytical methods that are vital to the national security of the United States; and (2) minimization procedures that carefully restrict access to the BR metadata and includes specific oversight requirements.[392]

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."[393]

Returning to the earlier point, in relation to FISC's abdication of its responsibilities: it was to protect U.S. persons' privacy interests that FISC was created in the first place. Congress did not anticipate that FISC would simply hand over this responsibility to the

---

[390] In re Production of Tangible Things *From* [REDACTED], Order, No. BR 08-13, at 2-3 (FISA Ct. Mar. 2, 2009), *available at* http://www.dni.gov/files/documents/section/pub_March%202%202009%20Order%20from%20FISC.pdf.
[391] *Id.* at 12.
[392] *Id.*
[393] *Id.*

NSA, once the NSA requested such a sweeping surveillance program that FISC lost the ability to conduct oversight.

C. Evisceration of Pen/Trap Provisions

All of the information obtained through the telephony metadata program is provided for in FISA's pen register and trap and trace provisions. In contrast to the process followed by the government with regard to section 215, however, the pen/trap provisions require prior targeting and limited collection of information. The use of second 215 to obtain seemingly limitless information amounts to an end-run around the pen/trap provisions.

D. Potential Violation of Other Provisions of Criminal Law

There are, in addition, other statutory provisions that raise question about the legality of the current telephony metadata program. Namely, in December 2008 FISC issued a Supplemental Opinion, noting 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.[394] The reason behind the document appears to be that although such orders were previously approved, for the first time the government cited 18 U.S.C.A. has identified the provisions of 18 U.S.C.A. §§2702-2703 as relevant to the question.

Under 50 U.S.C. §1861, Congress empowered the government to apply to the FISC "for an order requiring the production of *any* tangible things (including books, records, papers, documents, and other items."[395] 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."[396]

The Court had apparently considered "any" to be without limit, until 18 U.S.C.A. §§2702-2703 was brought to its attention. This statute laid out an apparently exhaustive set of circumstances under which telephone service providers could provide customer or subscriber records to the government.[397] An order under 50 U.S.C. §1861 was not included in this list. 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.[398]

---

[394] In re Production of Tangible Things From [REDACTED], Supplemental Opinion, No. BR 08-13 (FISA Ct. Mar. 2, 2009), *available at* http://www.dni.gov/files/documents/section/pub_Dec%2012%202008%20Supplemental%20Opinions%20from%20the%20FISC.pdf.

[395] 50 U.S.C.A. §1861(a)(1) (2006)(emphasis added).

[396] In re Production of Tangible Things From [REDACTED], Supplemental Opinion, No. BR 08-13, at 1 (FISA Ct. Mar. 2, 2009), *available at* http://www.dni.gov/files/documents/section/pub_Dec%2012%202008%20Supplemental%20Opinions%20from%20the%20FISC.pdf (citing United States v. Gonzales, 520 U.S. 1, 5 (1997); *accord* Ali v. Federal Bureau of Prisons, 128 S. Ct. 831, 836 (2008)).

[397] 18 U.S.C.A. § 2702(a)(3) (2013) (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"); 18 U.S.C.A. §2703(c)(1) (2013) ("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)).

[398] In re Production of Tangible Things From [REDACTED], Supplemental Opinion, No. BR 08-13, at 3 (FISA Ct. Mar. 2, 2009), *available at* http://www.dni.gov/files/documents/section/pub_Dec%2012%202008%20Supplemental%20Opinions%20from%20the%20FISC.pdf.

Judge Reggie 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 Congress, in the USA PATRIOT Act, 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.[399] Judge Walton pointed to the heightened requirements of §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. He then noted that §2703(c)(2) expressly permits the government to use administrative subpoenas to obtain certain categories of non-content information from a provider—and concluded that, surely, Congress could not have intended a higher standard for FISC orders.

The problem, of course, 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 §215, Congress nowhere includes in the language of 18 USC §§2703-2703 provision for FISC orders as an exception to the closed set. Instead, it allows 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.[400] The next paragraph, moreover, ties the provision directly to the actual commission of a crime. A court order for disclosure under §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."[401] The types of records being sought by the FBI from FISC, in contrast, extended well beyond records either relevant or material to an ongoing criminal investigation. Furthermore, under 18 USC §2703(d), the judiciary is empowered to quash or modify such orders where the records being requested "are unusually voluminous in nature."[402] 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.

VI. CONSTITUTIONAL CONSIDERATIONS

The government argues that the telephony metadata collection program complies with the Constitution.[403] In doing so, it relies on *Smith v. Maryland*, in which the 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. The government also argues that the national security interests at stake override whatever privacy intrusion arises from the bulk collection of telephony metadata.[404] These arguments are problematic.

The telephony metadata program amounts to a general warrant, the prohibition of which gave rise to the Fourth Amendment. Reliance on *Smith v. Maryland*, moreover is

---

[399] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA Patriot Act) of 2001, 18 U.S.C.A. § 2709(a) (2006).
[400] *Id.* at §2703(c)(2).
[401] *Id.* at §2703(d).
[402] *Id.*
[403] *See* Section 215 White Paper, *supra* note 223, at 3.
[404] *Id.*

misplaced: the case involved individualized, reasonable cause to believe that the target of the pen register had engaged in criminal behavior and threatening and obscene conduct. The placement of the pen register was obtained via consent. Significant technological and societal changes in the interim further render the third party doctrine a moot point. While lower courts might follow the Third Party Doctrine, the Supreme Court appears poised to recognize exceptions in light of modern interaction.

A. The Fourth Amendment Prohibition on General Warrants

At the time of the founding, English courts rejected general warrants. A different standard, however, marked the crown's 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.[405] 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."[406] 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."[407] Upon departure, the men seized Entick's documents, charts, pamphlets, and other materials.[408]

Chief Justice of the Common Pleas Charles Pratt, First Earl Camden, ruled that both the search and the seizure was unlawful. He explained:

> 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

---

[405] Entick v. Carrington, 19 Howell's State Trials 1029 (1765).

[406] The full warrant read:

> George Montagu Dunk, earl of Halifax, viscount Sunbury, and baron Halifax one of the lords of his majesty's honourable [sic.] 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 premisses, and further dealt with according to law; in the due execution whereof all mayors, sheriffs, justices of the peace, constables, and other majesty's officers 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, Dunk Halifax. To Nathan Carrington, James Watson, Thomas Ardran, and Robert Blackmore, four of the majesty's 'messengers in ordinary.'

Id.

[407] *Id.*

[408] *Id.*

> 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]?[409]

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.[410]

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."[411] The Court flatly rejected the use of such general warrants.

The use of writs of assistance 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.[412] As early as 1660 legislation to prevent Fraudes and Concealments of His Majestyes Customes and Subsidyes empowered magistrates to:

> [I]ssue out a Warrant to any person or persons thereby enableing him or them with the assistance of a Sheriffe Justice of the 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 open such Houses and to seize and secure the same goods soe concealed, and all Officers and Ministers of Justice are hereby required to be aiding and assisting thereunto.[413]

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 more strictly enforce trade and navigation laws –specifically, to "make the strictedst [sic.] and most diligent [sic.] Enquiry into the State of this dangerous and ignominious Trade."

---

[409] *Id.*
[410] *Id.*
[411] *Id.*
[412] 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).
[413] An Act to Prevent Fraudes and Concealments of His Majestyes Customes and Subsidyes, 12 Car. II, c. 19 (1660). *See also* Act for Preventing Fraudes and Regulating Abuses in his Majesties 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).

He ordered that every step authorized by law be taken "to bring all such heinous Offenders to the most exemplary and condign [sic.] Punishment."[414]

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 contrary to "the fundamental principles of law". Scholars hail Otis' argument in the case as helping "to lay the foundation for the breach between Great Britain and her continental colonies."[415] As A.J. Langguth observed, at the Writs of Assistance trial, "James Otis stood up to speak, and something profound changed in America."[416]

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.[417] In replying to Grindley, Otis stated that his efforts were being made "out of regard to the liberties of the subject." 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." He ignored the crown's claim of necessity—and current practice—noting that "the writ prayed for in this petition, being general, is illegal." He highlighted four concerns: first, it was universal—i.e., it could be executed by anyone in possession with 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 is the freedom of one's house," Otis opined. General warrants would annihilate the privilege associated with that right.[418]

Although the court ruled against Otis, John Adams later wrote that his arguments "breathed into this nation the breath of life."[419] Indeed, 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."[420] The Massachusetts Constitution of 1780 similarly objected to the use of general warrants:

---

[414] 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 407-08 (Samuel M. Quincy ed. (1865).

[415] LAWRENCE HENRY GIPSON, THE COMING OF THE REVOLUTION, 1763-1777 39 (1954).

[416] A.J. LANGGUTH, PATRIOTS: THE MEN WHO STARTED THE AMERICAN REVOLUTION 22 1998. For excellent studies of the case Otis argued see Gray, supra note 414, at 395-511; M. H. SMITH, THE WRITS OF ASSISTANCE CASE (1978); James M. Farrell, *The Child Independence is Born: James Otis and Writs of Assistance in* RHETORIC, INDEPENDENCE AND NATIONHOOD, Stephen E. Lucas ed., Vol. 2 of A Rhetorical History of the United States: Significant Moments in American Public Discourse (Martin J. Medhurst ed.).

[417] Farrell, *supra* note 416, at 16. *See also Paxton's Case of the Writ 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 (Samuel M. Quincy ed. (1865)

[418] Otis' speech is taken from L. KINVIN WROTH & HILLER B. ZOBEL, LEGAL PAPERS OF JOHN ADAMS VOL. 2 139-144 (1965). See also discussion in Farrell, *supra* note 416, at 19-22.

[419] THE WORKS OF JOHN ADAMS VOL. X. 276.

[420] Va. Decl. of Rights § 10.

> 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.[421]

The New Hampshire Constitution of 1784 lifted the clause almost verbatim.[422] The Virginia ratifying convention of 1788 made a point to ensure that the subsequent Constitution would incliude a provision affirming that "every freeman has a right to be secure from all unreasonable searches and siezures of his person, his papers and his property."[423] 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.'"[424] 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."[425] Madison understood the clause as a ban against general warrants.[426]

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 ot 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 fundmental principles of law, that ever 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

---

[421] Mass. Const. of 1780, pt. 1, art. XIV.

[422] New Hampshire Const. 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 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.

Id.

[423] EDWARD DUMBAULD, THE BILL OF RIGHTS AND WHAT IT MEANS TODAY 184 (1957), quoted in Akhil Reed Amar, *The Fourth Amendment, Boston, and the Writs of Assistance*, 30 Suffolk U. L. Rev. 53, 68 (1996).

[424] *Id.*, at 184, 191, 200-01, quoted and cited in Amar, *supra* note 423, at 68.

[425] *Id.*, at 207, quoted in Amar, *supra* note 423, at 68. (emphasis added). Note that the historical antecedent suggests a broad reading of the "persons, houses, papers, and effects" language of the Fourth Amendment.

[426] Thomas Y. Davies, *Recovering the Original Fourth Amendment*, 98 MICH. L. REV., 547, 555 (1999). *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 UNIV. OF COLORADO L. REV. 691, 692 (1982).

> 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 Idependence was born.[427]

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

> [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 th eBritish Constitution, and is quoted as such by the English authorities on that subject down to the present time.[428]

It was precisely general warrants that the Framers meant when referring to unreasonable searches and seizures.[429]

The Supreme Court has continued, throughout U.S. history, 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 is "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."[430] General warrants were presumptively unreasonable. To drive the point home, the first Congress, which started out with just one sentence outlawing unreasonable search and seizure, went on to add a second clause to the Fourth Amendment, requiring that no warrant shall issue but upon probable cause—ensuring in the process that government officials could not issue general warrants and still comport with the Fourth Amendment.

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."[431] Such a general warrant would immunize the officer who carried it out from a subsequent trespass suit.[432] In the case of *Entick v. Carrington*, "Armed with sweeping warrants issued by executive officials, various govenrment henchmen broke into Englishmen's houses, searched their papers, arrested their persons, and rummaged through their effects, in hopes of finding" wrongdoing.[433]

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."[434] 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."[435] Davies posits that the reason the Framers even bothered "to adopt constitutional bans against general warrants in light of the apparent

---

[427] Boyd v. United States, 116 U.S. 616, 624-25 (1886).
[428] *Id.* at 626.
[429] *Id.* at 627.
[430] Payton v. New York, 445 U.S. 573, 583 (1980).
[431] *See* Amar, *supra* note 423, at 60.
[432] *Id.*
[433] *Id.*, at 65.
[434] Davies, *supra* note 426, at, 551.
[435] *Id.*

consensus that the general warrant was illegal at common law" was because of genuine concern that Congress might edanger the right in the future.[436]

The FISC Order authorizing the telephony metadata program is, precisely, 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 activitiy. FISC admits that almost none of the information obtained relates to illegal behavior.

It matters little whether one stores ones papers in a filing cabinet in one's den, or places all financial documents on 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. Email, 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.

This is our modern day equivalent of the papers and effects held by Entick in his home, and allowing the govenrment to obtain records of all of this information is the equivalent of a digital trespass on our private lives.[437] The trespass in which the NSA is engaging is not supported by probable cause, it is not even supported by reasonable suspicion—indeed, no suspicion of any wrongdoing whatsoever is contemplated by the collection of myriad records of all U.S. persons. It is the equivalent of a general warrant and, as such, is odius to the Fourth Amendment.

B. Third Party Data

In defending the telephony metadata program, the government relies on the Court's construction of a reasonable expectation of privacy in *Katz v. United States* (1967) and argues that, consistent with *Smith v. Maryland* (1979) third party information is not constitutionally-protected. This argument fails to appreciate the fact pattern in *Smith v. Maryland*, the evolution of technology, and the manner in which society now operates. It also ignores that the shadow majority in *U.S. v. Jones* (2012), that suggests that the Supreme Court is moving to recognize the world in which we now live and to re-evaluate the level of protection afforded, consistent with the Fourth Amendment.

In 1967 the Supreme Court held that the Fourth Amendment protects people, not places.[438] Justice Potter Stewart, writing for Court, explained, "What a person knowingly exposes to the 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."[439]

---

[436] *Id*., at 657.

[437] Lord Camden explained in *Entick v. Carrington*:

> By the laws of England, every invasion of private property, be it ever so minute, is a trespass. No man can set his foot upon my ground without my license, but he is liable to an action, though the damage be nothing, which is proved by every declaration in trespass where the defendant is called upon to answer for bruising the grass and even treading upon the soil. If he admits the fact, he is bound to show, by way of justification, that some positive law has justified or excused him. The justification is submitted to the judges, who are to look into the books, and see if such a justification can be maintained by the text of the statute law, or by the principles of the common law. If no such excuse can be found or produced, the silence of the books is an authority, against the defendant, and the plaintiff must have judgment. According to this reasoning, it is now incumbent upon the defendants to show the law by which this seizure is warranted. If that cannot be done, it is a trespass.

See Entick v. Carrington, 19 Howell's State Trials 1029 (1765).

[438] Katz v. United States, 389 U.S. 347, 351 (1967) (citation omitted).

[439] *Id*.

The government suggests that a Section 215 order is not a "search" as to any person 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."[440] In the case in question, *Smith v. Maryland*, the 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.[441] The key sentence from the decision centered on the customer's relationship with the telephone company: namely "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties."[442] The government argues:

> Although the telephony metadata obtained through Section 215 includes, in addition to the numbers dialed, the length and time of the calls and other similar dialing, routing, addressing, or signaling information, under the reasoning adopted by the Supreme Court in Smith, there is no reasonable expectation of privacy in such information, which is routinely collected by telecommunications service providers for billing and fraud detection purposes.[443]

For the government, the breadth of the program does not convert the collection of bulk data into a search.[444] Further, the government argues that even if it were a search, it would still satisfy the reasonableness standard established by the Supreme Court to govern large-scale, but minimally intrusive suspicionless searches. Of particular importance here is the overriding government interest in protecting national security.[445]

The problem with the government's argument is that it glosses over some glaring differences between the bulk collection program and the facts of *Smith v. Maryland*. On March 5, 1976, Ms. Patricia McDonough was robbed in Baltimore, Maryland. 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. At one point, the caller asked her to go out in front of her house. When she did so, she saw the 1975 Monte Carlo moving slowly past her home. On March 16, the police observed a car of the same description in her neighborhood. Tracing the license plate, police discovered that the car was registered to Michael Lee Smith.[446]

The following day, the police asked the telephone company to install a pen register to trace the numbers called from Smith's home telephone. The company agreed, and that day Smith called Patricia McDonough's home. On the basis of this and other information, the police applied for and obtained a search warrant. Upon executing the warrant, police found a telephone book in Smith's home, with the corner turned down to Patricia McDonough's name and number. In a subsequent six-man lineup, McDonough identified Smith as the person who robbed her.[447]

---

[440] Section 215 White Paper, *supra* note 223, at 19.
[441] *Id.*, citing Smith v. Maryland, 442 U.S. 735, 743-46 (1979).
[442] Smith v. Maryland, 442 U.S. 735, 743-44 (1979).
[443] Section 215 White paper, *supra* note 223, at 20, citing in support SEC v. Jerry T. O'Brien, Inc., 467 U.S. 735, 743 (1984); United States v. Miller, 425 U.S. 435, 443 (1976).
[444] Section 215 White Paper, *supra* note 223, at 20 ("The scope of the program does not alter the conclusion that the collection of telephony metadata under a Section 215 court order is consistent with the Fourth Amendment. Collection of telephony metadata in bulk from telecommunications service providers under the program does not involve searching the property of persons making telephone calls. And the volume of records does not convert that activity into a search.")
[445] *Id.*, at 21.
[446] Smith v. Maryland, 442 U.S. 735 (1979).
[447] *Id*.

Although the police did not obtain a warrant prior to placing 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, placed the pen register consistent with their reasonable suspicion that Michael Lee 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, the Foreign Intelligence Surveillance Court acknowledges that almost all of the information thus 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 v. Maryland*, moreover, the police wanted only to record the numbers dialed from the suspect's telephone. 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.

In contrast, the bulk collection program now collects the numbers dialed, the numbers who call a particular number, trunk information, session times, and the like. And it has the ability to do that for not just one person, but for the entire country. Whereas the police in 1979 were concerned with whether Michael Lee Smith was calling a particular 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*. The sheer amount of information available is thus significantly different from what was at stake in the pen register placed on Michael Lee Smith's line.

Further characteristics distinguish the case. In 1979, the telephone company consented to placing the pen register on the line. Today, however, under the FISC order, telephone service providers are forced to comply with the government's request. Unlike the voluntary behavior that marked the case, the bulk collection program relies on coercive government power to obtain records on all telephone subscribers. And it is not for a limited time. In Smith v. Maryland, the police sought the information for an extremely limited period. The bulk metadata collection program has been operating for seven years now—and, the NSA argues—should be a permanent part of the government surveillance program.

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 information that can be learned about not just individuals, but neighborhoods, school boards, political parties, girl scout troops—indeed, any social, political, or economic network, is light years ahead of what the Court contemplated in 1979. The logic of the government's position has virtually no limit. Not only is telephony metadata more revealing than previously, but all forms of metadata are at stake.

Americans have a contractual relationship with myriad corporate entities now, to whom they have entrusted parts of their lives, such as friendships, corespondence, 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 than giving all information to the federal government. Americans reasonably expect that their movements, communications, and decisions will not be recorded and analyzed by the intelligence agencies. And a majority of the Supreme Court seems to agree.

In 2012 the Court considered a case involving 28-day surveillance. The government had 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. The day after the warrant expired, agents installed the device and followed the car's movements for nearly a month. Information thus obtained allowed the government to indict Antoine Jones and others on drug trafficking conspiracy charges.[448] 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.[449]

This case is important for determining the constitutionality of the telephony metadata program in two 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.[450]

Justice Scalia cited *Entick v. Carrington*, noting that the Court had previously 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."[451] 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 privacy against government that existed when the Fourth Amendment was adopted."[452]

Just as the Court eschewed the test in *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."[453]

The concept of a general warrant, and the Court's conception of the tort 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 ones 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 protections for privacy. 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.

Even though he adopted *Katz* as the relevant standard, Justice Samuel Alito, joined by Justice Ginsburg, Justice Breyer, and Justice Kagan, suggested that in most criminal

---

[448] United States v. Jones, 132 S. Ct. 945 (2012).
[449] *Id.* at 949.
[450] *Id.*
[451] *Id*.
[452] *Id*., at 947.
[453] *Id*. at 953.

investigations, long-term monitoring "impinges on expectations of privacy." 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.[454]

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."[455] 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 while 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."[456]

Justice Sotomayor went one step further. She suggested that, 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."[457] She 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.[458]

Justice Sotomayor 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."[459]

VIII. CONCLUDING REMARKS

The 1978 Foreign Intelligence 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,

---

[454] *Id.* at 963 (Alito, J., concurring).
[455] *Id*.
[456] *Id*. at 964.
[457] *Id*. at 957 (Sotomayor, J., concurring).
[458] *Id*.
[459] *Id*.

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 adopted by Congress in enacting FISA. The FISC orders lack the particularization required prior to the acquisition of information and the role FISC now plays departs from that envisioned by Congress. 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. 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, new technologies, and changed circumstances. An end to the telephony metadata program and FISA reform are necessary to bring surveillance operations and emerging technologies within the bounds of the Constitution.