Published in In *The Quest for Leadership: Essays in Honor of Thomas E. Cronin.* Michael Genovese, ed. (Amherst, NY: Cambria Press, 2015), pp. 131-148.

Presidents Bush, Obama and the Surveillance of Americans

James P. Pfiffner
School of Policy, Government, and International Affairs
George Mason University

The Framers of the Constitution created an independent executive in order to assure that there was a counterweight to potential congressional abuse of power and also to ensure that there would be an effective, single executive to implement the laws and public policy. In the 20th century the power of the executive increased considerably, particularly with respect to national security policy. That increase in power, has led at times to the abuse of power. Since the 1930s several presidents have undertaken surveillance of American citizens that pushed the boundaries of the law and the Fourth Amendment to the Constitution. Some of domestic surveillance and other abuses investigated in detail by the Church Committee, which in 1975 issued a report that detailed illegal surveillance of Americans by the CIA, FBI, and NSA, among other intelligence agencies. Such activities violated the privacy of hundreds of thousands of innocent US citizens in misguided attempts to protect the nation from "subversion."

Since the atrocities of 9/11, the US intelligence community has vastly expanded in size and scope; and with the growth of the internet, the technological capacity of the US government to collect information and communications of US citizens has increased exponentially. President George W. Bush initially authorized surveillance of Americans without the warrants required in law, based on his claimed inherent Article II powers. Congress later included some of these surveillance programs in law.

When Barack Obama was a Senator he asserted that President Bush exceeded his legitimate executive authority when he ordered surveillance of Americans without warrants. "The Supreme Court has never held that the president has such powers. As president, I will follow existing law, and when it comes to U.S. citizens and residents, I will only authorize surveillance for national security purposes consistent with FISA and other federal statutes."[1] But once he was in office, he embraced existing surveillance programs as necessary to protect US national security. When the extent of some of these programs was unveiled by Edward Snowden in the summer of 2013, people concerned with civil liberties expressed alarm at their scope.

[1] Charlie Savage, "Barack Obama's Q & A," *Boston Globe* (December 20, 2008). **http://www.boston.com/news/politics/2008/specials/CandidateQA/ObamaQA/**

After briefly noting some of the abuses that the Church Committee uncovered in the 1970s, this chapter will examine three intelligence surveillance programs that continued under President Obama and the potential threats to privacy and civil liberties that they present. Collecting foreign intelligence and domestic intelligence that is directly related to national security is essential. The danger, however, is that in the enthusiasm to ferret out foreign intelligence, agencies will collect much more information on innocent Americans than is necessary, and that accumulation of communications and information will tempt future leaders to use it for political or partisan purposes rather than for strictly national security purposes.

I. The Church Committee, FISA, and the President's Surveillance Program

The Church Committee, in its review of domestic intelligence activities of the federal government from 1936 to 1976, drew the lesson that "History Repeats Itself." In its investigations it found that every president from Franklin Roosevelt to Richard Nixon had received from US intelligence agencies information about domestic activities that were purely political and not related to foreign intelligence or national security. Intelligence was compiled on the "Women's Liberation Movement," (sic) Martin Luther King, the NAACP, the John Birch Society, Senator Adlai Stevenson, Congressman Abner Mikva, and many other political groups and individuals. The NSA, CIA, FBI, and the Army compiled dossiers on hundreds of thousands of individuals including information from first class letters, private telegrams, tax returns, and telephone calls. [2]

The Church Committee Report went into great detail about large scale intelligence programs and concluded: "We have seen a consistent pattern in which programs initiated with limited goals, such as preventing criminal violence or identifying foreign spies, were expanded to what witnesses characterized as 'vacuum cleaners,' sweeping in information about lawful activities of American citizens. The tendency of intelligence activities to expand beyond their initial scope is a theme which runs through every aspect of our investigative findings."[3] History is repeating itself again in the vast collection of domestic communications by the National Security Agency. The communications of Americans who are not the targets of surveillance and who are not suspected of any wrongdoing were compiled by NSA, and the danger is that these data bases may be used for purposes not connected with national security. After the abuses of domestic surveillance revealed in the Church Committee hearings of 1975, Congress passed the Foreign Intelligence Surveillance Act to prevent such abuse in the future.

After the attacks of 9/11, President Bush initiated surveillance programs that authorized NSA to collect data on US citizens. Though initially conducted without orders from the Foreign Intelligence Surveillance Court, the program was changed and authorized by amending the USA PATRIOT ACT in 2006. Section 215 of the Patriot Act was reinterpreted to allow bulk collection of metadata on US citizens' communications, making legal what had been previously prohibited by law. Section 702 of the amended Foreign Intelligence Surveillance Act allows the

---

[2] *U.S. Senate Select Committee on Intelligence Activities Within the United States* (Church Committee Report) 1975, reprinted by Red and Black Publishers (St. Petersburg, Florida, 2007), pp. 22, 11-13.

[3] Church Committee Report, p. 9.

targeting of non-US persons "reasonably believed" to be outside the United States for purposes of foreign intelligence.[4] Under section 702 the content of calls, in addition to the metadata, can be collected. (Senator Obama voted to reauthorize the Patriot Act in 2006 and the 2008 FISA Amendments.) In addition, President Reagan's 1981 Executive Order 12333 can be interpreted to authorize NSA to collect information on US persons if their electronic communications are stored in computers outside the United States. Critics say that this may be a backdoor way of collecting the content of US phone calls and other data that cannot be legally collected under the auspices of Sections 215 or 702.

Critics of US surveillance policies argue that Section 702 of FISA, Section 215 of the Patriot Act, and Executive Order 12333 allow the surveillance of persons in the US about whom the NSA, CIA, or FBI have no suspicion of illegal connection with foreign powers. Thus the surveillance of and storage of data about presumably innocent persons without warrants arguably violates the Fourth Amendment to the Constitution, which guarantees that "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated and no Warrants shall issue, but upon probable cause. . . ." The following sections will examine the civil liberties issues involved in these three authorizations.

Creation of FISA

Before 1978 presidents authorized wiretaps and searches concerning national security based on their own executive and national security authority. After the abuses uncovered by the Church Committee, Congress passed the Foreign Intelligence Surveillance Act (FISA), which was designed to codify the use of national security surveillance within the United States. The Act created the Foreign Intelligence Surveillance Court (FISC) to review surveillance programs, judge their legality, and issue orders (in effect, warrants) to surveil individuals believed to be connected to foreign powers.

The law applied to domestic surveillance, and leaves the president free to conduct any foreign surveillance (of foreign persons) that he thinks necessary. Edward Snowden's release of classified National Security Agency (NSA) documents in June 2013 raised concerns about the extent of electronic surveillance and data collection of Americans' communications. Initially, the FISC authorized governmental surveillance only with respect to specific persons or places. But beginning in 2004 it interpreted the law to authorize bulk collection of telephone metadata.[5]

[4] Privacy and Civil Liberties Oversight Board, "Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act (as amended), July 2, 2014, p. 4.

[5] Privacy and Civil Liberties Oversight Board, "Report on the Telephone Records Program Conducted under Section 215 of the PATRIOT Act and on the Operations of the Foreign Intelligence Surveillance Court (January 23, 2014), p. 13.

Origins of the President's Surveillance Program[6]

Less than a month after 9/11, on October 4, 2001, President Bush, through the President's Surveillance Program (PSP), authorized the National Security Agency to monitor communications related to foreign intelligence that were coming into or going out of the United States. Ordinarily, communications passing into or out of the United States via wires or cables would have required a FISC order. But President Bush proceeded based on his interpretation of his constitutional authority as president.

The President's Surveillance Program included four types of collection:

1) Bulk telephone metadata
2) Contents of telephone calls
3) Internet communications
4) Bulk collection of internet metadata[7]

After a legal analysis of the President's Surveillance Program in March 2004, the Office of Legal Counsel of the Justice Department decided that the first three programs were legal under the president's order, but that the fourth, bulk collection of internet data, was not legal. This finding led to a crisis in which Assistant Attorney General James Comey (acting for Attorney General John Ashcroft, who was in the hospital), along with other political appointees and career lawyers in the Justice Department threatened to resign if the illegal program was reauthorized by the president against its recommendation.[8]

When President Bush was told by Comey of the possible resignations, he suspended the program for a short period of time, beginning March 26, 2004.[9] Once the program was suspended, DOJ and NSA began to search for another legal basis for the program. By July 14, 2004 Chief FISC Judge Kollar-Kotelly had determined that the bulk collection of internet data could be justified by Pen Register/Trap Trace authority.[10] With a few minor changes, the PP/TT

---

[6] This section is based on Office of the Inspector General of the National Security Agency, Central Security Service, Working Draft ST-09-0002 (24 March 2009), classified TOPREFORM, SECRET//STLW//COMINT/ORCON/NOFORN http://www.scribd.com/doc/162439434/090324-Draft-NSA-IG-Report-Working-Draft-Office-Of-The-Inspector-General-NSA-24-March-2009.

[7] Laura K. Donohue, "FISA Reform", Georgetown Law, (The Scholarly Commons, 2014), p. 4; http://scholarship.law.georgetown.edu/facpub/1318/. NSA Inspector General Report, p. 37.

[8] For an account of these incidents, see James P. Pfiffner, *Power Play: The Bush Administration and the Constitution* (Washington: Brookings, 2008), pp. 182-189.

[9] NSA Inspector General Report, p. 38.

[10] A pen register records dialing or other outgoing signals from a phone or other communications mechanism. Trap and trace records all incoming electronic data to a communications device. PR&TT does not include content of communications. See Laura K. Donohue, "Bulk Metadata Collection: Statutory and Constitutional Considerations," *Harvard Journal of Law and Public Policy*, Vol. 37, p. 796.

allowed NSA to continue to collect the same internet metadata it had under the PSP. The internet metada program itself was ended in 2011 because it was not seen as operationally effective.[11]

By January, 2007 the other three programs, foreign content order, the business records order (telephony metadata), and the domestic content order were reauthorized under new FISC orders, and thus their legality did not depend alone on the President's Article II authority.[12]

II. Section 702 of FISA: Collecting Content of Communications

Electronic surveillance of Americans for national security purposes inside the US since 1978 required a warrant ("order") from the Foreign Intelligence Surveillance Court (FISC) based on probable cause that the person was an "agent of a foreign power."[13] Section 702 of FISA authorized NSA to obtain the contents of communications without a warrant only if the "target is reasonably believed to be a non-US person located outside the United States."[14] The language of the Patriot Act was meant to allow NSA to use roving wiretaps to follow a suspect who changed phones or carriers. But between 2005 and 2007 the USA Patriot Act was reinterpreted to broaden its scope. The word "facility" traditionally meant a specific phone number or email address; but DOJ and NSA reinterpreted the word to include a "general gateway" or "cable head." This would allow NSA to collect all of the communication content passing through the routers of telecommunication companies.[15] This change tremendously increased the scope of communications that could be gathered and stored under Section 702.

The PRISM program, beginning in 2007 after FISA was amended, allowed NSA to directly tap into the central servers of internet companies and collect "audio, video, photographs, e-mails, documents" and "collect all traffic crossing Internet cables – not just information targeted at specific Internet Protocol (IP) addresses or telephone numbers."[16]

NSA is allowed to compile "incidental" information on US persons whose communications are collected in the process of targeting foreign persons, though Americans' identity must be "minimized." In collecting intelligence on foreign persons, there is no need for probable cause, and if information on US persons is collected with them, the communications of Americans can be stored and queried. The problem, according to scholar Laura Donohue is that in "post-targeting analysis" the intelligence community can "query data obtained under Section 702, effectively bypassing protections Congress introduced to prevent reverse targeting." She

---

[11] Robert O'Harrow Jr. and Ellen Nakashima, "President's Surveillance Program worked with private sector to collect data after Sept. 11, 2001," *Washington Post* (June 27, 2013).
[12] NSA Inspector General Report, pp. 38-39.
[13] President's Review Group, *Liberty and Security in a Changing World*, Report and Recommendations of the President's Review Group on Intelligence and Communications Technologies (December 12 ,2013), p. 67.
[14] PCLOB Report, (January 23, 2014), p. 1.
[15] Donahue, "Section 702," pp. 17-21.
[16] Laura K. Donohue, "Section 702 and the Collection of International Telephone and Internet Content," Georgetown University Law Center (2014) forthcoming *Harvard Journal of Law and Public Policy*, Vol. 38 (2015), p. 5.

argues that such use of US persons data "falls outside the reasonableness component of the Fourth Amendment."[17]

The Privacy and Civil Liberties Oversight Board (PCLOB) was created in law as an independent, bipartisan agency in the executive branch. Its mission is "to analyze and review actions" by the executive branch and ensure that there is an appropriate balance "with the need to protect privacy and civil liberties;" and to "ensure that liberty concerns are appropriately considered" in the implementation of policies to prevent terrorism.[18]

In its report of July 2014, the PCLOB concluded that the "core" of the 702 program is "clearly authorized by the FISA statute. The requirements also "fit[s] within the totality of the circumstances' standard of reasonableness under the Fourth Amendment." Furthermore, it has been successful in gathering intelligence about potential terrorist attacks, playing a "Key role in discovering and disrupting specific terrorist plots."[19] The Board found no signs of wrongdoing, but it found that some aspects of 702 Program "push the program close to the line of constitutional reasonableness." Such as:

1) the large scope of "incidental collection of U.S. persons' communications"
2) "use of 'about" collection, of messages neither to nor from the target"
3) "use of queries to search for specific US persons"[20]

One of the Board's concerns was that communications of US persons collected inadvertently (incidentally) are not purged from databases, even if there is no direct connection to foreign intelligence.[21]

One problem with the "incidental" collection of the content of communications from foreign sources is that they remain in the PRISM database. From NSA's perspective, since no probable cause is required to collect foreign communications, no probable cause is necessary to query the database for names of Americans in the US. According to deputy assistant attorney general, Brad Wiegmann, "Once we've collected it [the evidence], we've gotten the necessary court approvals," and do not need further authorization to query whatever is already in the NSA database.[22] The Board recommended better assessment of the collection involving US persons and also limits on using US persons as identifiers. It recommended that NSA should query the system for specific US persons only if there is documentation that the search is "reasonably likely to return foreign intelligence information."[23]

In August 2013 President Obama, prompted by disclosures by Edward Snowden of the extent of NSA surveillance of Americans, created a special President's Review Group on

---

17 Donohue, "Section 702," pp. 8-9.
18 PCLOB Report (January 2014), p. 2.
19 PCLOB Report (July 2014), pp. 9-10.
20 PCLOB Report (July 2014), p. 9
21 PCLOB Report (July 2014), p. 8.
22 H.L. Pohlman, "Querying the FISA Queries," *Washington Post*, (April 7, 2014).
23 PCLOB Report (July 2014), p. 12.

Intelligence and Communications Technologies. The task of the group was to provide advice as to how US policy could "not only . . . protect against threats" but also safeguard the "right to privacy, "which is essential to a free and self governing society" and "the long-term vitality of American democracy."[24]

The Review Group was more critical than the government Privacy Oversight Board and was particularly concerned about large scale storage of communications of Americans that was collected "incidentally" to surveillance of foreign targets. It recommended that "if the government legally intercepts communication under section 702, or under any other authority that justified the interception of a communication on the ground that it is directed at non-United States person who is located outside the United States," that the information on US persons be purged when it is discovered, that it not be used in legal proceedings, and that the government not examine the contents of legally obtained communications in order to identify a US person.[25]

If the NSA wanted to directly target Americans, it would have to get an order from the FISC. But communications to or from Americans who were not targeted could be collected and queried without any warrant or order. According to Gellman, et al., "The NSA treats all content intercepted incidentally from third parties as permissible to retain, store, search and distribute to its government customers."[26]

NSA told the FISA Court that it did not monitor domestic communications, but some of the documents revealed by Edward Snowden provided evidence that thousands of communications of Americans in the United States were in its database. Reporter Barton Gellman of *Washington Post* did an analysis of the leaked NSA documents collected under the Section 702 program.[27] The *Washington Post* staff went through 160,000 messages from the period 2009-2012 (including email and instant-messaging), 7,900 documents, and 11,000 on line accounts. The documents indicated that 10,000 US account holders were included in the database and were recorded and retained, even though they were not targeted. The data included 5,000 photographs, medical records, and love letters that were mostly not relevant according to NSA personnel.[28] The communications of these persons were considered to be incidental data and thus could be queried in NSA searches.

Senator Ron Wyden (D-Ore), a member of the Senate Intelligence Committee criticized the NSA's use of 702 program data. "When Congress passed Section 702 back in 2008, most

---

[24] President's Review Group, pp. 11-12.

[25] President's Review Group, (Recommendation 12, pp. 28-29). The "any other authority" referred to Executive Order 12333 was a reference to Executive Order 12333 (John Napier Tye, "Meet Executive Order 12333: The Reagan rule that lets the NSA spy on Americans," *Washington Post* (July 18, 2014).

[26] Barton Gellman, Julie Tate, and Ashkan Soltani, "In NSA-intercepted data, those not targeted far outnumber the foreigners who are," *Washington Post*, July 5, 2014.

[27] Gellman, et al., "NSA-intercepted data."

[28] Gellman, et al., "NSA-intercepted data."

members of Congress had no idea that the government was collecting Americans' communications simply because they contained a particular individual's contact information."[29] In a statement, Senators Wyden and Mark Udall (D-Colo) criticized the NSA:

> It is now clear to the public that the list of ongoing intrusive surveillance practices by the NSA includes not only bulk collection of Americans' phone records, but also warrantless searches of the content of Americans' personal communications, including emails. . . . Senior officials have sometimes suggested that government agencies do not deliberately read Americans' emails, monitor their online activity or listen to their phone calls without a warrant. However, the facts show that those suggestions were misleading, and that intelligence agencies have indeed conducted warrantless searches for Americans' communications using the 'back-door search' loophole in section 702 of the Foreign Intelligence Surveillance Act.[30]

Massive amounts of information on Americans stored in NSA databases raises the possibility that the information might be abused in the future.[31]

III. Section 215 of the Patriot Act: collecting metadata

Section 215 of the USA PATRIOT Act, as interpreted by the Foreign Intelligence Surveillance Court, allows NSA to collect "metadata" from virtually all telecommunications companies' phone records in the United States. Metadata includes the time and place of a call, the recipient and duration of the call. Section 215 does not allow content of calls to be recorded.

Metadata can be very revealing, even if the content of communications is not recorded. According to former NSA General Counsel Stewart Baker, "metadata absolutely tells you everything about somebody's life. If you have enough metadata, you don't really need content.[32] According to Michael Hayden, former Director of NSA and later CIA, the information gained from metadata can be extremely accurate and informative: "we kill people based on metadata. But that's not what we do with this [domestically acquired] metadata." He continued, "it's really important to understand the program in its entirety. Not the potentiality of the program, but how

---

[29] Ellen Nakashima and Barton Gellman, "Court gave NSA broad leeway in surveillance, documents show," *Washington Post,* (June 30, 2014).

[30] Udall, Mark, "Revelations that Intelligence Agencies Have Exploited Foreign Intelligence Surveillance Act 'Loophole,'" *National Journal* (April 1, 2014); http://www.nationaljournal.com/library/133751.

[31] Despite declarations by some members of Congress that they did not know the extent of NSA surveillance, top level NSA officials say that Congress was informed. It could be that only the intelligence committees were informed or that members did not take the time to examine classified documents.

[32] Quoted in Alan Rusbridger, "The Snowden Leaks and the Public," *New York Review of Books*, (Nov. 21, 2013); http://www.nybooks.com/articles/archives/2013/nov/21/snowden-leaks-and-public/.

the program is actually conducted."[33] But the potentiality of the program is what worries those concerned with civil liberties. Even if none of the data is being misused in the present, a future president or executive branch worker or contractor could use the personal metadata to thwart political adversaries or for personal reasons.

From the huge database of metadata stored by the NSA, queries can be made of particular persons or numbers, foreign or domestic, as long as there is a "reasonable, articulable suspicion" (RAS) that there is some association with terrorism. In addition to the specific number queried, the requester can access the information on those numbers which have had contact with that number ("contact chaining"). In this process the "first hop" consists of those people who were in contact with the number under suspicion. The "second hop" includes numbers that were in contact with those in the first hop and the third hop all those who were in contact with the second hop numbers.[34]

Privacy and Civil Liberties Oversight Board Report

In January of 2014 the PCLOB issued a report that severely criticized the legal basis for the FISC interpretation of section 215 of the Patriot Act. According to the PCLOB, the intent of business records part of Section of 215 of the Patriot Act was to allow the FBI to access the records of businesses that were relevant to an investigation. The Board argued that the bulk collection of metadata cannot be "relevant" to a specific FBI investigation in any meaningful way. The operation of the program compelled telephone companies to pass through data to NSA on a daily basis, rather than search their own records for specific persons or numbers.

According to the PLOC Board, the FISC, in defense of its ruling, has maintained "that essentially the entire nation's calling records are 'relevant' to every counterterrorism investigation. . . . This position is untenable. Moreover, the interpretation . . . is dangerously overbroad, leading to the implication that virtually all information may be relevant to counterterrorism and therefore subject to collection by the government. . . . At its core, the approach boils down to the proposition that essentially all telephone records are relevant to essentially all international terrorism investigations."[35] "This is an approach lacking foundation in the statute."[36]

The bulk collection of telephony metadata is antithetical to the purposes of FISA. FISA was created to preclude the types of surveillance programs that before 1978, collected data on hundreds of thousands of Americans without a specific showing that their actions were suspect.[37] FISA attempted to protect Americans' privacy by requiring that *before* surveillance was

---

[33] Lee Ferran, "Ex-NSA Chief: 'We Kill People Based on Metadata,'" (May 12, 2013). http://abcnews.go.com/blogs/headlines/2014/05/ex-nsa-chief-we-kill-people-based-on-

[34] PCLOB Report, January 2014, p. 9.

[35] PCLOB Report, January 2014, p. 60.

[36] PCLOB Report, January 2014, p. 57.

[37] For instance Project MINARET, COINTELPRO, Operation CHAOS, and Operation SHAMROCK; see the Church Committee Report, passim; and Donohue, "Bulk Metadata," p.772-774.

conducted, there had to be a *specific suspect*, that there was *probable cause* for the suspicion, and that the FISA Court would judge the request for the warrant ("order").[38] Thus Section 215 reverses the purpose of FISA. Instead of *first* finding probable cause that a specific person is connected to a foreign power and *then* investigating that person, Section 215 allows NSA to *first* collect masses of data on virtually all US telephone messages, and *then* search for possible suspected activity.[39]

The bulk collection of metadata is dubious for both legislative and constitutional reasons. Almost by definition, bulk metadata cannot be "relevant to an authorized investigation," since the data are collected in bulk and do not pertain to a specific investigation. In effect, the 215 program amounts to a general warrant, which is specifically rejected by the Fourth Amendment to the Constitution.[40]

Some members of Congress were not aware of the reinterpretation of Section 215 of the Patriot Act, and became vocally critical of its use. Congressman James Sensenbrunner, who was a supporter of the Patriot Act, said that he did not know about how DOJ and NSA were interpreting section to collect bulk metadata on Americans. "Recently, I have gone on record seeking to illustrate the large gap between the intention of the Patriot Act and the implementation of Section 215 by the FISA court and the Administration." He said that Section 215 constituted "an abuse of that law," and that "both the administration and the FISA court are relying on an unbounded interpretation of the act that Congress never intended."[41] He also introduced a bill that would end NSA's bulk collection of metadata (the USA Freedom Act).[42]

The Effectiveness of Section 215

The PCLOB found that the 215 program has had "minimum value" in protecting the United States and that NSA representatives "have not identified a single instance involving a threat to the United States" that was thwarted by use of the data; nor has the program led to "the discovery of a previously unknown terrorist plot or the disruption of a terrorist attack."[43] The PCLOB concluded that there are "serious" dangers for privacy and civil liberties in the continued collection of phone metadata based on Section 215. It argued that the routine collection of all US calls "fundamentally shifts the balance of power between the state and its citizens." With governmental powers of compulsion, the program is in danger of "mission creep," and that collected personal information might be used to "harass, blackmail, or intimidate, or to single out for scrutiny particular individuals or groups."[44] Despite finding no evidence of current abuse of

---

[38] Laura K. Donohue, "Bulk Metadata Collection: Statutory and Constitutional Considerations," *Harvard Journal of Law and Public Policy*, Vol. 37 (2014), pp. 763-767.
[39] Donohue, "Bulk Metadata Collection," p. 805.
[40] Donohue, "Bulk Metadata Collection, p. 898.
[41] Statement of Complaint for ACLU vs. Clapper (June 11, 2013) US District Court Southern District of New York [13 CIV 3994].
[42] James Sensenbrenner, 2013 "Jim's Weekly Column" June 17, 2013; http://sensenbrenner.house.gov/news/documentsingle.aspx?DocumentID=339292.
[43] PCLOB Report, January 2014, p. 11.
[44] PCLOB Report, January 2014, p. 12.

the data collected in the program, the Board judged that there was a significant chance of a "chilling effect" on the First Amendment rights of freedom of speech and association.

By majority vote, the Board recommended ending the bulk collection of metadata under section 215.[45] It argued that in the case of suspected terrorism, the government could use traditional court warrants to investigate suspected activity; it does not need the phone metadata on all US telephone calls in order to protect the country from terrorism.

IV. Executive Order 12333

While FISA controls intelligence surveillance within the United States, Executive Order 12333, issued by President Reagan in 1981, established authority to gather intelligence outside the United States.[46] If communications are collected outside the United States and those communications include the "incidental" collection of communications of Americans, the information can be stored by NSA and later queried with a US name identifier. Thus if American internet companies back up or store their data in servers located in foreign countries, information on large numbers of Americans can be swept up. Some critics argue that NSA personnel can avoid any constraints of Section 702 of FISA and Section 215 of the Patriot Act by using the data collected under Executive Order 12333 authority to examine US persons' communications.[47]

John Napier Tye, a former State Department official filed a "whistle blower complaint" with the NSA Inspector General and the Senate and House intelligence committees, arguing that the collection and storage of data on Americans under the authority of Executive Order 12333 violated the Fourth Amendment. He explained his actions by saying, "It's a problem if one branch of government can collect and store most Americans' communications, and write rules in secret on how to use them – all without oversight from Congress or any court."[48]

The President's Review Group, Recommended (Number 12) that, ". . . if the government legally intercepts communication under section 702, or under *any other authority* (emphasis added) that justifies the interception of a communication on the ground that it is directed at non-United States person who is located outside the United States," the information should be "purged upon detection" unless it is directly relevant to a legitimate inquiry. They also recommended that the evidence not be used in criminal cases, and that the government not be allowed to search for a particular person unless it is directly related to foreign intelligence.[49] The "any other authority" referred to in the recommendation was Executive Order 12333.[50]

---

[45] PCLOB Report, January 2014, p. 16.
[46] President's Review Group, p. 70, 73-76.
[47] Charlie Savage, "Reagan-Era Order ton Surveillance Violates Rights, Says Departing Aide," *New York Times* (Aug. 13, 2014).
[48] John Napier Tye, "Meet Executive Order 12333: The Reagan rule that lets the NSA spy on Americans," *Washington Pos*t (July 18, 2014).
[49] President's Review Group, 2013, pp. 28-29.
[50] John Napier Tye, "Meet Executive Order 12333: The Reagan rule that lets the NSA spy on Americans," *Washington Post* (July 18, 2014).

The President's Review Group concluded: "there have been serious and persistent instances of noncompliance in the Intelligence Community's implementation of its authorities."[51] Further, "the government should not be permitted to collect and store mass, undigested, non-public personal information about US persons for the purpose of enabling future queries and data-mining for foreign intelligence purposes."[52] This conclusion applies to Executive Order 12333 as well as to Section 215 of the Patriot Act.

Conclusion

One basic difference between defenders of mass collection of surveillance data and its critics is their differing time perspectives. Defenders of collecting bulk data argue that there are rigorous, executive branch constraints in place and that the programs are not used for illegitimate surveillance of Americans. As Michael Hayden said, "In this debate, it's important to distinguish what might be done with what is being done." Readers of the NSA Inspector General report and other documents will realize that NSA legal regulations are taken seriously. And critics of the programs are often willing to concede that the programs are not being abused in the present. But the danger is that in the future, politicians (such as Lyndon Johnson or Richard Nixon) or lower level workers will be tempted to use the data available to them for high-minded purposes to protect the country from dissident or for low-minded partisan political purposes.

Just a brief glance at the history of government surveillance in the United States -- from the Alien and Sedition Act of 1789, to Palmer Raids after World War I, to the internment of Japanese Americans during World War II, to the red scare of the 1950s, to the Johnson and Nixon administrations' surveillance of political dissenters, to the post-9/11 surveillance of Americans – should be enough to convince anyone that there is a natural tendency of law enforcement agencies to overreact to perceived threats. The pressure on presidents to protect the nation from harm – and to avoid a terrorist attack on *their* watch – is tremendous. To protect the nation is an implicit promise that presidents make, and in the case of terrorism, overpromising is inherent because of public expectations. Americans have high, and often unrealistic, expectations of presidents. Thus it is important for Congress, the judiciary, and the citizenry to maintain vigilant to ensure that presidents do not overstep constitutional constraints.

* The author would like to thank Bob Deitz, Michael Hayden, and Harold Pollman for comments on an earlier draft of this chapter. The analysis and conclusions are mine alone.

* James P. Pfiffner is University Professor in the School of Policy, Government, and International Affairs at George Mason University. He has written or edited sixteen books and more than 100 articles and chapters on the presidency, public administration and American national government. He has been a visiting scholar at the School of Advanced Study at University College London and Griffith University in Brisbane Australia. His recent books include *Power Play: The Bush Presidency and the Constitution* (Brookings 2008) and *Torture as Public Policy* (Paradigm Publishers, 2010).

---

[51] President's Review Group, 2013, p. 76.
[52] President's Review Group, 2013, p. 108.