Issues in
Governance Studies

Number 68 March 2015

Secrecy and negligence: How Congress lost control of domestic surveillance

by William Bendix and Paul J. Quirk

William Bendix is an assistant professor of political science at Keene State College. His research focuses on Congress, legislative deliberation, and homeland security and civil liberties policies.

Paul J. Quirk is the Phil Lind Chair in U.S. Politics and Representation at the University of British Columbia and a former research associate at the Brookings Institution. His work focuses on debate and deliberation in Congress and the mass public.

EXECUTIVE SUMMARY

In enacting the USA PATRIOT Act just weeks after the 9/11 terrorist attacks, Congress sought to enhance investigations against specific, named persons suspected of terrorism. As voluminous documents leaked by whistleblower Edward Snowden have revealed, however, the president and the National Security Agency (NSA) have relied on that law to authorize the daily, ongoing capture of all U.S. communication records. These documents make clear that the Bush and Obama administrations ignored statutory constraints to authorize exceptionally broad intelligence-gathering programs. But from our review of legislative hearings and debates on the PATRIOT Act over the last five years, along with numerous declassified documents on surveillance, we find that unilateral action by the executive branch was only partly to blame for unrestrained domestic spying.

After the relatively balanced and cautious provisions of the 2001 PATRIOT Act, Congress virtually absented itself from substantive decision making on surveillance. It failed to conduct serious oversight of intelligence agencies, ignored government violations of law, and worked harder to preserve the secrecy of surveillance practices than to control them. Even after the Obama administration made the essential facts about phone and email surveillance available in classified briefings to all members, Congress mostly ignored the information and debated the reauthorizations on the basis of demonstrably false factual premises. Until the Snowden revelations, only a handful of well-briefed and conscientious legislators—too few to be effective in the legislative process—understood the full extent of domestic intelligence gathering.

We describe and explain Congress's deliberative failure on phone and Internet surveillance policy. We show that along with a lack of consistent public concern for privacy, and the increasing tendency toward partisan gridlock, Congress's institutional methods for dealing with secret surveillance programs have undermined its capacity to deliberate and

act effectively with respect to those programs. Although the current political environment is hardly conducive to addressing such problems, we discuss long-term goals for institutional reform to enhance this capacity. We see no easy or decisive institutional fix. But without some structural change, the prospects look dim for maintaining significant limitations on investigatory intrusion in an era of overwhelming concern for security.

...[A]long with a lack of consistent public concern for privacy, and the increasing tendency toward partisan gridlock, Congress's institutional methods for dealing with secret surveillance programs have undermined its capacity to deliberate and act effectively with respect to those programs.

INTRODUCTION

In drafting the original PATRIOT Act mere weeks after the traumatic security failure of the September 11 attacks, Congress sought to expand and improve protections against terrorism. But, contrary to much of the political lore, it also showed serious concern for privacy safeguards. The House Judiciary Committee, controlled by Republicans, pushed for only a limited expansion of investigative powers and insisted that most surveillance provisions in the PATRIOT Act expire after four years unless reauthorized. The sunset provisions were intended to ensure a serious review of the new surveillance practices to determine whether sufficient privacy protections were in place. Yet, 12 years later, as documents made public by Edward Snowden revealed, the NSA was sweeping up and analyzing vast amounts of U.S. communication records, or "metadata," without observing significant constraints. The Snowden documents also showed that the Foreign Intelligence Surveillance Court (FISA) had radically reinterpreted the PATRIOT Act, in secret, to permit bulk collection of phone records. Paradoxically, while the incidence of terrorism has been much lower in the years after 9/11 than anyone expected, government surveillance has been much more intrusive than legislators authorized. What happened? Why did Congress so thoroughly fail to exercise control and ensure effective protection of privacy? What are the lessons for future policymaking?

During the last five years of legislative debates over the PATRIOT Act, Congress has failed to define or control surveillance policy. Prior to the Snowden leaks, most members had little awareness of NSA activities and Congress had little capacity to impose constraints. Now, more than 18 months after Snowden exposed the mass seizure of phone records, not much has changed. To a great extent, the source of difficulty has been the inadequacy of the institutional arrangements for legislative deliberation on secret programs. Some members have declined opportunity to learn about domestic-spying practices, while others have opposed placing restrictions on the NSA for fear of giving terrorists any tactical advantage.

If Congress had conducted thorough, informed deliberations at all stages, we suspect it would have endorsed extensive collection of communication records, but it would have also imposed limitations and constraints to minimize the harm to privacy interests. Instead, it gave the executive branch essentially unfettered authority to operate a massively intrusive program.

CONGRESS AND SURVEILLANCE POLICY: GENERAL CONSIDERATIONS

Our account of the development of the metadata surveillance programs centers on Congress and its interactions with several institutions—the president, the FISA Court, and the Justice Department, among others—and proceeds through several phases. We begin with brief theoretical remarks on the central institutional properties that drive the account.

We argue that Congress as an institution has great difficulty acting in any consistent, balanced way to protect privacy interests on surveillance issues. On one hand, when setting broad priorities in general terms, it attaches considerable weight to privacy interests. On the other hand, when faced with specific issues of investigatory authority, it readily makes sweeping, indiscriminate sacrifices of those same interests—even without distinct evidence of serious threat.

The lack of consistency in defending privacy interests has several sources. Most fundamental, legislators reflect the attitudes and demands of their constituencies. The American public has generally been quite willing to surrender privacy rights for the sake of enhanced security, against even unspecified, highly indefinite terrorist threats.[1] In addition, there are generally no well-organized, powerful constituencies for privacy interests.[2]

But several factors exaggerate the effect. First, decisions on surveillance are largely about risk (for example, the probability of an abusive "fishing expedition" versus that of a major terrorist attack). Congress members have strong temptations to defer to the executive branch on decisions that could, therefore, turn out badly. Second, the president's party is more interested in defending the executive than in checking its decisions.[3] Third, surveillance politics is complicated by long-term partisan and ideological divisions that were shaped by the particular conflicts of the Cold War era. For generations, the main targets of intelligence-agency surveillance have been mostly on the political left. This history may inhibit the response of many Republicans to the threat of intrusive government, even though the main targets and likely victims of intrusive surveillance are no longer a well-defined ideological category. Fourth, the committee system has been another impediment:

1 Clem Brooks and Jeff Manza, *Whose Rights? Counterterrorism and the Dark Side of American Public Opinion* (New York: Russell Sage Foundation, 2013).

2 Amy B. Zegart, *Eyes on Spies: Congress and the United States Intelligence Community* (Stanford, CA: Hoover Institution/Stanford University Press, 2011).

3 Thomas E. Mann and Norman J. Ornstein, *The Broken Branch: How Congress Is Failing America and How to Get It Back on Track* (New York: Oxford University Press, 2006), p. 155.

overlapping jurisdictions among the Homeland Security, Intelligence, and Judiciary panels prevent any one of them from being held accountable for stalled policy or lapses in oversight.[4]

Finally, and very important, Congress has particular difficulties with policies that must be decided in secret—such as those for controlling technologically advanced surveillance methods. To prevent profuse leaks, Congress and the executive have imposed severe restrictions on members' access to information. When the full House or Senate decides policy, however, the restricted information encourages some members to opt out of serious participation, degrading the intelligence of deliberation and promoting deference to the executive.

Lacking any settled disposition on surveillance issues, Congress will respond to the leadership, and sometimes merely the political cover, provided by other institutions—especially the president, the intelligence agencies, and the FISA Court. It may take cues from the Justice Department or other executive agencies, and it will defer to rulings by the regular federal courts. In the end, Congress's performance in protecting privacy may depend on the design of the legislative arrangements for dealing with secret programs and on the structures and missions of relevant administrative and judicial institutions.

THE PATRIOT ACT AND BUSINESS RECORDS

The legal basis for the NSA's phone metadata program is the business-records provision of the PATRIOT Act.[5] But the legislative history of this provision, consisting of multiple revisions, shows that lawmakers never intended to permit such a program. In fact, Congress demonstrated a serious concern for privacy interests each time it revised the measure.

Congress first created business-records orders in 1998, three years before the PATRIOT Act. These orders allowed federal agents to collect a suspect's receipts from hotels, motels, storage facilities, and vehicle-rental companies.[6] To obtain approval for the orders, Justice Department lawyers, working on behalf of the Federal Bureau of Investigation (FBI), had to demonstrate to the FISA Court that a suspect was linked to a foreign government or organization; they did not have to show that the target had engaged in espionage or terrorism.[7] This evidentiary standard was intended to be low, so that agents could obtain documents with relative ease at the beginning of cases to identify or eliminate suspects quickly.

The failure to prevent the 2001 terrorist attacks pushed Congress to expand existing surveillance

4 Sean Gailmard, "Multiple Principals and Oversight of Bureaucratic Policy-Making," *Journal of Theoretical Politics* 21:2 (2013), pp. 161-186; see also Mann and Ornstein, *The Broken Branch*, pp. 151-158.

5 Section 215 of the USA PATRIOT Act (P.L. 107-56).

6 Section 602 of the Intelligence Authorization Act for Fiscal Year 1999 (P.L. 105-272).

7 Michael J. Woods, "Counterintelligence and Access to Transactional Records: A Practical History of USA PATRIOT Act Section 215," *Journal of National Security Law and Policy* 1 (2005), pp. 37-71.

powers by passing the PATRIOT Act. Among its many sections, the act included a provision for enhanced business-records orders.[8] No longer limited to a narrow set of receipts, investigators could now serve an order to any type of business and obtain "any tangible things"—including books, papers, computers, and other electronic devices—deemed relevant to a terrorism investigation. The provision also stipulated that authorities no longer had to show evidence that the target had affiliation with a foreign group. Agents could simply gather private records on anyone whose activities they considered, for whatever reason, pertinent to a terrorism or intelligence case.[9]

Concerned about the possibility of investigative abuse, however, lawmakers set the business-records provision to expire in December 2005. Congress reviewed the use of records requests before the legislative sunset took effect and decided, in early 2006, to renew the business-records provision but with a higher evidentiary standard. Under the new law, FISA applications now needed to include a "statement of facts" demonstrating that the items sought were somehow connected to a suspected foreign agent, raising the evidentiary standard close to the 1998 version.[10] In addition, Congress placed a new four-year sunset on the business-records provision to ensure another review of the measure in 2009.

Although the shifting evidentiary standards for records requests created a complex body of law, two points stand out. First, in all versions of the business-records provision, Congress made clear that orders were to be used against a specific individual in a particular ongoing investigation. Legislators never contemplated bulk-collection orders that lacked named targets and that permitted the capture of records for cases yet to be launched. Second, in both the PATRIOT Act and its 2006 reauthorization, Congress specified that business-records orders were to be used by the FBI. Neither bill mentioned the NSA. As we discuss next, secret interpretations of the PATRIOT Act authorizing dragnet collection of metadata overlooked the statutory restrictions.[11]

EXECUTIVE ACTION AND THE METADATA PROGRAMS

In the decade between the PATRIOT Act's passage and Snowden's first leaks, Congress played no part in developing or modifying the NSA's domestic programs. In fact, aside from the limited involvement of two FISA Court judges, the Bush and Obama administrations made all decisions over blanket-collection procedures. But Congress did not opt out of deliberations and policy formulation. The executive simply ignored surveillance restrictions included in the PATRIOT Act and decided to

8 Section 215 of the PATRIOT Act.

9 Mary DeRosa, Andrew C. McCarthy, and Peter P. Swire, "Section 215: Access to Business Records under FISA ('Libraries Provision'); Section 214: Pen Register and Trap and Trace Authority under FISA," in *Patriot Debates: Experts Debate the USA PATRIOT Act*, eds. Stewart A. Baker and John Kavanagh (Chicago: American Bar Association, 2005), pp. 47-63.

10 Section 106 of the USA PATRIOT Improvement and Reauthorization Act of 2005 (P.L. 109-177).

11 Privacy and Civil Liberties Oversight Board, Report on the Telephony Records Program Conducted under Section 215 of the USA PATRIOT Act on the Operations of the Foreign Intelligence Surveillance Court (Washington, DC: U.S. Department of Justice, 2014), p. 10. From here on cited as PCLOB.

keep nearly all legislators, except for congressional leaders and four members on the Intelligence committees, in the dark.[12]

On October 4, 2001, as legislators drafted the PATRIOT Act, President Bush authorized the bulk collection of Internet and phone metadata in secret and without congressional approval.[13] The Internet metadata program enabled the NSA to gather billions of online communication records between U.S. persons. It tracked email messages from the sending to the receiving accounts, apparently without capturing their content. Similarly, the phone metadata program collected the numbers for all incoming and outgoing calls made within the United States. With data stockpiled for five years, NSA analysts could potentially map out large social networks that included terrorism or espionage suspects. But they could also, if they so chose, use the data to pry into the personal affairs of innocent Americans.

Despite his willingness to make unilateral decisions, Bush wanted a legal rationale for the bulk collection of communication records. Thus White House lawyers argued in a memo that Congress had granted Bush new, expansive powers when it passed an authorization of force against al-Qaeda shortly after 9/11.[14] Among these new powers, they claimed, was the president's authority to order domestic surveillance without having to inform or seek approval from the FISA Court.[15] These arguments, although highly questionable, satisfied NSA officials and lawyers. And in November 2001, after the installation of hidden computer servers, AT&T, Verizon, and BellSouth began supplying the NSA with communication records daily. The Justice Department secretly reauthorized the dragnet programs every one or two months.[16]

With the stored data, NSA analysts could try to identify new suspects by entering search terms—such as phone numbers associated with terrorist groups—into a massive database. The initial search target, called the "seed," was often obtained from an alert list compiled by an automated software system.[17] Initial queries would reveal all phone numbers or email addresses in direct contact with, or one "hop" from, the seed. But analysts would routinely do additional searches to

12 From publicly available accounts, it appears that the Bush administration briefed the so-called Gang of Eight—i.e., House and Senate leaders, as well as chairs and ranking members on the Intelligence panels—when the programs were first launched. For example, after assuming the top Democratic position on the Senate Intelligence Committee in 2003, Jay Rockfeller (D-WV) learned of the metadata programs from Vice-President Dick Cheney. See Ryan Lizza, "State of Deception; Why won't the President rein in the intelligence community?" *The New Yorker* (December 16, 2013).

13 On the same day, Bush also authorized the Terrorist Surveillance Program, which allowed the NSA to conduct warrantless eavesdropping on U.S. calls and emails involving out-of-country participants. Information collected under the metadata and warrantless-surveillance programs was codenamed Stellar Wind.

14 The Authorization for Use of Military Force (P.L. 107-40).

15 Apparently, it first informed the presiding judge of the FISA Court about the metadata programs in 2002. It informed the other ten members of the Court in 2006. See David S. Kris, "On the Bulk Collection of Tangible Things," *Journal of National Security Law & Policy* 7 (2014), p. 212, n 18.

16 Lizza, "State of Deception."

17 This system scanned all new numbers that were added to NSA databases, identifying ones of possible interest and adding them to the alert list for analysts to investigate further. See PCLOB, p. 47.

identify all numbers within three hops from a seed. By one estimate, a single search involving three hops would potentially allow analysts to identify over 400,000 contacts.[18]

In 2004, after conducting a new legal review of the metadata programs, Justice Department officials refused to reauthorize the email dragnet—forcing Bush to suspend Internet collection and seek approval from the FISA Court. The basis for the belated resistance remains unknown. But whatever the reasoning, this decision had little impact on NSA surveillance. A few months later, in closed proceedings of the FISA Court, Presiding Judge Colleen Kollar-Kotelly approved the bulk collection of Internet data.

Kollar-Kotelly decided that bulk collection was permissible because the PATRIOT Act allowed investigators to capture any email records that were "relevant" to a terrorism case. Since all email metadata were potentially relevant, they could be scooped up by the NSA.[19] Although siding with the government, Kollar-Kotelly stipulated that analysts could not examine the captured data indiscriminately. A search could only be initiated after NSA administrators had reviewed evidence and found a "reasonable articulable suspicion" that an email account had an "association with" terrorist activity. And analysts could only gather and evaluate communication records on accounts that were within two hops from the seed.[20] In 2011, because of NSA violations, including the collection of message contents without warrants, the FISA Court rescinded its approval of the Internet metadata program.[21] But before withdrawing its support, the Court used the same rationale and conditions it had applied to the email dragnet to authorize the ongoing seizure of phone data.[22]

The Bush administration had asked the FISA Court to sanction the bulk collection of U.S. phone records in 2006. The administration sought judicial approval because phone companies, concerned that they would be vulnerable to lawsuits if details of the program ever leaked, threatened to withhold records unless they received court orders.[23] In its application, the administration argued that approval of a phone metadata program would be "consistent" with the FISA Court's earlier authorization of the email records program.[24] Judge Malcom Howard of the FISA Court agreed, signing an order that approved the administration's application. Howard's order cited the business-

18 PCLOB, p. 165.

19 She cited Section 214 of the PATRIOT Act, which authorizes the use of pen registers and trap-and-trace devices. See Opinion and Order, No. PR/TT [redacted] [Foreign Intelligence Surveillance Court], p. 48.

20 Ibid., p. 83.

21 The Obama administration has repeatedly stated that it ended the email metadata program after the Court's ruling. See Devlin Barrett, "Surveillance Court Judge Criticized NSA 'Overcollection' of Data," *The Wall Street Journal* (August 11, 2014).

22 PCLOB, pp. 39-40.

23 In December 2005, *The New York Times* reported on the NSA's warrantless recording of U.S. calls under the Terrorist Surveillance Program. These reports, apparently, prompted the phone companies to seek explicit court approval for all metadata collection.

24 Memorandum of Law in Support of Application for Certain Tangible Things for Investigations to Protect Against International Terrorism, In *re Application of the Federal Bureau of Investigation for an Order Requiring Production of Tangible Things*, No. BR 06-05 (Foreign Intelligence Surveillance Court) (May 23, 2006), p. 3.

records provision, which Congress had recently reauthorized, noting that it allowed for the seizure of "tangible things." Otherwise, the order provided little legal justification for the decision.[25] But it did stipulate that many restrictions imposed on the email metadata program now be applied to the bulk collection of phone records.[26]

The reauthorization thus gave Congress the opportunity to respond to the vast executive-branch expansion of phone and email surveillance. But Congress neither sought to reassert the privacy protections of the existing business-records provisions—forcing an end to the dragnet programs—nor attempted to establish legislative standards to regulate the collection and use of metadata. In effect, Congress surrendered control to the executive branch.

In all the discussions on bulk collection between the White House and the FISA Court, Congress was absent. This absence resulted initially from the Bush administration's overt decision to exclude legislators. But once legislators gained opportunity to learn about and shape surveillance policy, a combination of indifference and deception in Congress ensured that most members remained absent from the debate.

THE CONGRESSIONAL RESPONSE: DEFERENCE AND AVOIDANCE

By the time the PATRIOT Act came up for its second renewal in 2009, the executive branch had abandoned the strategy of secrecy and unilateralism on the metadata programs. Starting in 2007, after the dragnets had received court approval, the Bush administration provided full and regular disclosures to the Intelligence and Judiciary committees.[27] Going further, the Obama administration made repeated efforts to provide all members of Congress, through secret briefings, with the essential information on the metadata programs.[28] The reauthorization thus gave Congress the opportunity to respond to the vast executive-branch expansion of phone and email surveillance. But Congress neither sought to reassert the privacy protections of the existing business-records provisions—forcing an end to the dragnet programs—nor attempted to establish legislative standards to regulate the collection and use of metadata. In effect, Congress surrendered control to the executive branch.

25 See Order *re Application of the Federal Bureau of Investigation for an Order Requiring Production of Tangible Things*, No. BR 06-05 (Foreign Intelligence Surveillance Court) (May 24, 2006), p. 3. Importantly, the FISA Court did not issue a full legal justification of the phone metadata program until 2013. See PCLOB, p. 100.

26 PCLOB, pp. 43-46.

27 Kris, "On the Bulk Collection of Tangible Things," p. 259.

28 PCLOB, pp. 97-99.

Congress's passivity partly reflected the incentives of individual members to defer to the executive and avoid the security and political risks of imposing constraints on investigatory methods. But the restricted flow of information on secret intelligence capabilities and practices also contributed heavily. Most legislators did not attend classified briefings—some because they lacked interest in surveillance policy, others because they were intentionally excluded from meetings by congressional leaders. A few highly engaged members, mostly Democrats, made use of the executive briefings to become well informed. But these members could not speak publicly about the actual practice of bulk collection and, as a result, could not make an effective case for policy change. Meanwhile, leading members who wanted to protect the metadata program from legislative interference took advantage of the widespread ignorance to misrepresent business-records orders as narrowly-focused investigative tools. As the later reaction to the Snowden leaks made clear, most members remained serenely clueless about metadata collection.

Congress in the end opted for two short-term extensions before reauthorizing the business-records provision, without change, until June 2015. The debates over renewal stretched over three years, from 2009 to 2011, giving the appearance of thorough deliberation. But that appearance was utterly false. While maintaining the secrecy of the metadata program, Congress failed to assess the security value of mass records seizures, to weigh the resulting harm to privacy interests, or to impose standards or requirements to minimize that harm.

THE 2009 REAUTHORIZATION

The 2009 round of congressional debates, which led ultimately to a one-year extension of the PATRIOT Act, revealed frustrations over the deliberative process among members of both parties. But the sources of frustration differed between Republicans and Democrats.

On the one hand, House Republicans, in the minority, saw no reason to hold prolonged discussions of investigative tools that they considered unproblematic. They disapproved of the short-term extension and pushed to make the business-records provision permanent, claiming that years of extensive oversight by Congress had revealed no evidence of agents violating privacy rights with FISA Court orders. Rep. Daniel Lungren (R-CA) insinuated that most members sought a short-term extension merely because they were uncomfortable supporting the unpopular PATRIOT Act. "Forgive me," he said during a debate, "but it almost sounds like we're treating it [reauthorization] like a burp after a big meal, something we're kind of embarrassed about."[29]

On the other hand, Senate Democrats were unable to discuss the main reasons why, in their view, the PATRIOT Act needed to be substantially amended. In an open hearing, Senate Judiciary Chairman Patrick Leahy (D-Vt.) awkwardly criticized the FISA Court rulings on the metadata programs without revealing the nature of the programs—complaining that the court had applied "a

29 *Congressional Record* 156 (February 10, 2010), H847.

presumption of relevancy."[30] Senator Russ Feingold (D-Wis.) noted that "critical information about implementation of the PATRIOT Act has not been made public—information that I believe would have a significant impact on the debate."[31] In a floor statement, he went further: "Section 215 [i.e., the business-records provision] has been misused. I cannot elaborate, but I believe that the public deserves some information about this."[32] He added that a group of senators had pressed the Obama administration to declassify the secret uses of records requests, but that the administration had refused.

Feingold's statement revealed that some members of Congress were engaged in closed-door deliberations over domestic surveillance. We do not have direct reports on those discussions. As a result of the Snowden leaks, however, we know a good deal about the classified briefings and the information they provided to members. The Intelligence and Judiciary panels had access to all FISA documents and reports, and they were briefed regularly about the dragnets.[33] In contrast with Bush, the Obama administration took steps to involve all members of Congress in the debate over metadata collection. It prepared a five-page letter on the business-records provision and the NSA bulk programs, and instructed the intelligence panels to provide all House and Senate members access to the letter before any reauthorization vote.[34]

Nevertheless, we have grounds for skepticism about the effectiveness of those closed-door deliberations. We do not know what questions were asked, what claims were made, or what materials were presented in the closed sessions. Moreover, and perhaps more important, we do not know how many members read the Obama letter or sought information from intelligence officials or the committees. But as we discuss later, most members apparently failed to learn about the metadata programs until the Snowden leaks—indicating that the procedures for classified deliberations did not succeed in providing the essential information to a critical mass of members.

THE 2011 EXTENSION AND REAUTHORIZATION

Congress passed a ten-month extension of the business-records provision, followed by a four-year reauthorization, in 2011.[35] This round of debates over the PATRIOT Act echoed the 2009 round of deliberations, with many Republicans again pushing to make the records provision permanent and with some Democrats again calling for revisions to the measure. Between these two rounds of

30 Reauthorizing the USA PATRIOT Act; Ensuring Liberty: Hearing before the Subcommittee on Administrative Oversight and the Courts of the Committee on the Judiciary United States Senate, 111th Congress, 1st Session (September 23, 2009), p. 10.

31 Ibid., p. 16.

32 *Congressional Record* 156 (February 25, 2010), S793.

33 Kris, "On the Bulk Collection of Tangible Things," pp. 257-260.

34 Letter from Assistant Attorney General Ronald Weich to the Honorable Silvestre Reyes, Chairman, Permanent Select Committee on Intelligence United States House of Representatives (December 14, 2009).

35 FISA Sunsets Extension Act of 2011 (P.L. 112-003); PATRIOT Sunsets Extension Act of 2011 (P.L. 112-014).

debates, however, political conditions had undergone a major change that affected the breadth of discussions. In the 2010 midterm election, Republicans had won majority control of the House by gaining sixty-three seats. Many of these freshman Republicans identified with the Tea Party, viewed all government power with deep suspicion, and opposed the PATRIOT Act.[36] To minimize potential difficulties, Republican leaders rushed deliberations on surveillance policy, ensuring that discussions were less informed, less accurate, and less thorough than the limited debates two years earlier.

As in 2009, the Obama administration provided a letter to Congress that explained the metadata programs, their legal basis, and the FISA Court's oversight role.[37] The administration again gave copies of the briefing letter to leaders of the Intelligence panels and asked them to make it available to all members of Congress before a reauthorization vote. The Senate Intelligence Committee under Diane Feinstein (D-Calif.) complied, giving all senators opportunity to read the letter in early 2011. But the House Intelligence Committee, under Chairman Mike Rogers (R-Mich.), withheld the letter from many Republicans, especially freshmen.[38] As a result, these members only learned about the NSA dragnets when *The Guardian* and *The Washington Post* published the first Snowden leaks in June 2013. We do not know why Rogers suppressed the letter, but he may have feared that new members would oppose extension if they knew the expansiveness of domestic surveillance.

In addition to concealing classified information, Republican House leaders omitted hearings and markups and restricted floor debate to rush passage of the business-records extensions. Rep. Jim Sensenbrenner (R-Wis.), one of the authors of the original PATRIOT Act, defended the truncated process, arguing that Congress had debated FISA Court orders at length in previous years. "The time for multiple temporary extensions is over," he declared, calling for a permanent reauthorization.[39] He dismissed Tea Party resistance to the bills as uninformed "scare-mongering."[40]

At the same time, Intelligence Chairman Rogers and Judiciary Chairman Lamar Smith (R-Texas) made the false assertion that the extensions merely continued to provide antiterrorism agents with the same tools that criminal investigators had. Business-records orders, they claimed, were used to seize the very same documents as grand jury subpoenas.[41] What they omitted from their explanation was that authorities used FISA Court orders to seize data on millions of calls per day—something that investigators could never do with subpoenas.

---

36 Robert Draper, *Do Not Ask What Good We Do: Inside the U.S. House of Representatives* (New York: Free Press, 2012).

37 Letters from Assistant Attorney General Ronald Weich to the Honorable Dianne Feinstein and the Honorable Saxby Chambliss, Chairman and Vice Chairman, Senate Select Committee on Intelligence; and to the Honorable Mike Rogers and the Honorable C.A. Dutch Ruppersberger, Chairman and Ranking Minority Member, Permanent Select Committee on Intelligence U.S. House of Representatives (February 2, 2011).

38 It is unclear who among House Democrats, aside from members of the Judiciary and Intelligence panels, had access to the briefing paper. See PCLOB 2014, p. 98; Brendan Sasso, "Amash: Intelligence Committee Withheld Surveillance Document from House," *The Hill* (August 12, 2013).

39 *Congressional Record* 157 (February 8, 2011), H521.

40 *Congressional Record* 157 (February 14, 2011), H737.

41 *Congressional Record* 157 (February 14, 2011), H733.

Following Republican leaders in the House, Democratic leaders in the Senate scheduled no hearings or markups on the reauthorization bills and used procedural tricks to limit floor discussion on the four-year extension. Leahy pushed to raise the evidentiary standard for business-records orders, while Senators Ron Wyden (D-Ore.) and Mark Udall (D-Colo.) offered an amendment designed to declassify the phone metadata program. But Majority Leader Harry Reid (D-N.V.) filled the amendment tree to block these proposals from the floor.

With no way to modify the bill, Wyden and Udall nonetheless spoke at length against surveillance policy during debate over the four-year extension. Before the final vote on the reauthorization, Wyden gave a 23-minute floor speech that included stark warnings about the secret interpretation of the law and chastised the Senate for the members' ignorance:

> When the American people find out how their government has secretly interpreted the PATRIOT Act, they are going to be stunned and they are going to be angry. They are going to ask senators: Did you know what this law actually permits? Why didn't you know before you voted on it?....[M]any members of Congress have no idea how the law is being secretly interpreted by the executive branch…. It is almost as if there are two PATRIOT Acts, and many members of Congress have not read the one that matters.[42]

Disregarding these warnings, Congress extended the business-records provision until June 1, 2015.[43]

Overall, ignorance and misinformation marred congressional deliberations on the renewal of the business-records provision. Prominent members, including committee chairs, made specious claims to suggest that records requests had a limited scope, much like subpoenas in criminal probes. These comparisons reinforced the general view that agents only used FISA Court orders in traditional types of investigations where only one or a few suspects were targeted. Opponents could not refute these inaccurate statements without exposing the classified metadata program, and thus they faced an insurmountable deliberative challenge: to persuade colleagues of privacy violations without identifying the nature of the violations or providing any evidence of them. Wyden's speech presented the sharpest, most detailed rebuttal. But the many members who had not attended classified briefings lacked a basis for evaluating Wyden's claims against the many assurances from committee chairs that the PATRIOT Act authorized only modest, uncontroversial surveillance tools.

Two years later, the Snowden leaks demonstrated the breadth and depth of Congress's ignorance during the 2011 debates. Among members who did not sit on the regularly briefed committees, many expressed shock and outrage over the revelations. They readily admitted that they had not attended

42 *Congressional Record* 157 (May 26, 2011), S3386.

43 PATRIOT Sunsets Extension Act of 2011 (P.L. 112-014).

classified briefings offered by the Obama administration.[44] Worse, members on the Intelligence and Judiciary panels acknowledged that they had lacked understanding of the metadata program. They found the briefings overly technical, frequently evasive, and loaded with undocumented claims about the successes of bulk collection.[45] As Rep. Jan Schakowsky (D-Ill.), a member of the House Intelligence Committee, confessed after the leaks, "In terms of the oversight function, I feel inadequate most of the time."[46] In an egregious case of legislative malfeasance, a senior House Judiciary Committee Republican, Jim Sensenbrenner, who had helped lead the push for permanent authorization, claimed that he had attended no classified briefings and had had no knowledge of the metadata program prior to the leaks.[47]

In the debates, supporters of the PATRIOT Act had insisted that the business-records provision needed to be extended, without change, because FISA Court orders provided investigators with invaluable information. Yet when the leaks revealed the metadata program, these supporters had difficulty producing evidence of its effectiveness. Senator Feinstein, for example, asserted that "54 terrorist events have been interrupted" since 9/11 because of NSA surveillance.[48] But two reports, by two separate executive-branch panels, noted that these plots were largely disrupted by aggressive surveillance overseas, not by bulk collection in the United States.[49] Even the NSA has admitted that the program's effectiveness has eroded in recent years, because it only captures about 30 percent of all call records due to rapidly increasing cellphone use.[50] The phone dragnet may have yielded important leads, but Congress has offered no evidence of such benefits.

In short, the Snowden revelations exposed a profound failure by Congress to understand and deliberate about the government's massive collection of phone and email records. It dealt with the need for secrecy by leaving the decisions entirely to the president or the intelligence agencies themselves, while pretending to maintain statutory standards.

44 Tim Starks, "Intelligence Oversight Split on Access between Haves, Have-Notes," *Congressional Quarterly/Roll Call* (June 10, 2013).

45 Peter Wallsten, "Lawmakers Say Obstacles Limited Oversight of NSA's Telephone Surveillance Program," *The Washington Post* (August 10, 2013).

46 Quoted in ibid.

47 Adam Serwer, "PATRIOT Act Architect Cries Foul on NSA Program, but Skipped Briefings," *MSNBC* (June 13, 2013), available at http://www.msnbc.com/msnbc/patriot-act-architect-cries-foul-nsa-progr.

48 Diane Feinstein, "NSA's Watchfulness Protects America," *The Wall Street Journal* (October 13, 2013).

49 For example, the Privacy and Civil Liberties Oversight Board examined the fifty-four cases cited by Feinstein and found that only twelve involved the collection of U.S. records. Of those twelve cases, the Board reported that "we have not identified a single instance involving a threat to the United States in which the telephone records program made a concrete difference in the outcome of a counterterrorism investigation. Moreover, we are aware of no instance in which the program directly contributed to the discovery of a previously unknown terrorist plot or the disruption of a terrorist attack." See PCLOB 2014, p. 146.

50 Ellen Nakashima, "NSA Is Collecting Less than 30 Percent of U.S. Call Data, Officials Say," *The Washington Post* (February 7, 2014).

POST-SNOWDEN STALEMATE

The Snowden revelations, resulting in a yearlong series of scandalous front-page news stories, led to widespread demands for legislative action. The leaked documents largely eliminated the problems of deliberating a secret program by making it no longer secret. But ongoing security concerns and ever-increasing partisan gridlock have prevented Congress from acting.

Soon after the revelations, members in the House and Senate offered proposals to end metadata collection. Entitled the USA FREEDOM Act, the bills would require phone providers to retain customer logs for five years rather than have the NSA seize and stockpile them. For investigators to examine a suspect's call history, they would need to obtain a FISA Court order. A majority of House Republicans passed a bill with strong Democratic support in May 2014, but Republicans filibustered the Senate bill six months later. The different outcomes in the two chambers were the result of the rising threat posed by the Islamic State of Iraq and Syria (ISIS) in the spring and summer of 2014, and of important differences between the House and Senate bills.

Although both versions prohibited a countrywide dragnet, the House bill included broad permissive language that might allow the NSA to collect all call records in a given city or state. The Senate bill, by contrast, made it clear that the agency would be limited to seeking the records of individual suspects.[51] Many House Republicans apparently supported the House bill precisely because it called for only modest policy change. If the stronger bill had passed the Senate, House Republicans would probably have rejected any House-Senate compromise that imposed major constraints on metadata collection.

The fragility of congressional concern for privacy was apparent. Critics of the Senate's USA FREEDOM bill made one overriding argument—that weakening surveillance programs now would enable terrorists, especially ISIS, to successfully attack the United States. During floor debate, Senator Marco Rubio (R-Fla.) warned that a "gutted" surveillance program could lead to "a horrifying result."[52] And Senator Susan Collins (R-Maine) asked, "Why would we weaken the ability of our intelligence community at a time when the threats against this country have never been greater?"[53] These critics offered no evidence of the investigative value of the phone dragnet, and simply omitted mentioning considerations of privacy.

---

51 A major difference between the two bills was how they defined "selection term"—that is, the information initially used by the NSA to start a metadata search. Section 107 of the House bill (H.R. 3361) defined the selection term as "a discrete term, such as a term specifically identifying a person, entity, account, address, or device, used by the Government to limit the scope of the information or tangible things sought." Privacy advocates worried that the FISA Court could interpret "address" to mean state, city, or zip code, and thus let the NSA seize and examine tens of millions of call records for a single investigation. Section 107 of the Senate bill (S. 2685) used the same definition for selection term. However, it went on to define address as a particular physical location or a particular email account. And it also specified that a search term could not be based on "a broad geographic region, including a city, State, zip code, or area code." See Harley Geiger, "Why We Can't Support the New USA FREEDOM Act," *Just Security* (May 21, 2014), available at http://justsecurity.org/10689/guest-post-support-usa-freedom-act/.

52 *Congressional Record* 160 (November 18, 2014), S6077.

53 Ibid., S6078.

These debating points demonstrate the rhetorical advantage of concern for security, over that for privacy, in surveillance policy: the dangers of terrorist attacks are obvious and salient; those of intrusive surveillance are speculative and invisible. In the current environment, not only do many members simply accept the executive and FISA Court nullification of the statutory limits on business-records seizures, they reject all legislative constraints on the collection, storage, and use of phone metadata.

The future of NSA's dragnet is uncertain. With the business-records provision set to expire in June, the current legal basis for the metadata program will lapse unless Congress passes another reauthorization. Partisan gridlock on the issue makes a new surveillance law doubtful, and it raises the possibility of the NSA having to restore the far more restricted pre-9/11 procedures. But legislative inaction in 2015 might not end the NSA metadata programs, even if it ended their current statutory basis. For one thing, the FISA Court might approve bulk collection of communication records by reinterpreting one or more permanent provisions of the PATRIOT Act, much as it did earlier with the business-records provision. Alternatively, it could stretch an obscure provision in the PATRIOT Act that appears to permit, indefinitely, new business-records orders for terrorism investigations that predate the June 1 sunset—simply by defining those investigations in very broad terms.[54] Supporters of the metadata program may still press for a bill that authorizes the business-records provision permanently, but they may not regard the June 2015 sunset as a critical deadline for accomplishing it.[55]

Even if Congress at some point enacted new restrictions on surveillance, the executive might ignore the law and continue to make policy unilaterally. The job of reviewing

...[L]egislative inaction in 2015 might not end the NSA metadata programs, even if it ended their current statutory basis. For one thing, the FISA Court might approve bulk collection of communication records by reinterpreting one or more permanent provisions of the PATRIOT Act, much as it did earlier with the business-records provision. Alternatively, it could stretch an obscure provision in the PATRIOT Act that appears to permit, indefinitely, new business-records orders for terrorism investigations that predate the June 1 sunset—simply by defining those investigations in very broad terms.

54 Charlie Savage, "N.S.A. Phone Data Collection Could Go On, Even if a Law Expires," *The New York Times* (November 20, 2014).

55 Benjamin Wittes, "On the Oddity of the PATRIOT Act Sunset Provisions," *Lawfare* (November 24, 2014), available at http://www.lawfareblog.com/2014/11/on-the-oddity-of-the-patriot-act-sunset-provisions/.

executive conduct would again fall to the FISA Court.[56] In view of this court's history of broad deference to the executive, Congress would have a challenge to ensure that legislative policies were faithfully implemented.

REFORMING SURVEILLANCE POLICYMAKING

Ideally, in the aftermath of the Snowden scandals, Congress would undertake to restore order and legal regularity to surveillance policy by passing new legislation on the metadata program. Conceivably, it could choose to end bulk collection of phone records and reaffirm the original requirement of individual orders for the seizure of a target's business records. Given the prevailing sense of urgency about antiterrorism security, however, we think a constructive measure would more likely sanction metadata collection, subject to conditions and requirements designed to avoid unnecessary harm to privacy interests.

For the immediate future, however, Congress appears to have gone out of the business of determining policy for antiterrorism surveillance. In the near term, the best hope for privacy interests is for President Obama to make good on his post-Snowden pledge, repeated in his 2015 State of the Union Address, to reform surveillance programs in order to instill "public confidence…that the privacy of ordinary people is not being violated." He promised to work with Congress on the issue. If Congress is not capable of acting, the executive branch can impose its own constraints on surveillance practices.[57] But the maintenance of self-imposed executive-branch constraints would depend entirely on the strength of the administration's commitment—and, in two years' time, on the disposition of the next president. Because of the president's central responsibility for national security, the presidency is hardly a reliable institutional champion for privacy interests.

If over the long run surveillance practices are to afford significant protection to privacy interests, Congress will need to overcome its partisan gridlock and strengthen the institutional framework for surveillance policymaking. We suggest two long-term goals. First, Congress should seek some means of enhancing its capacity for oversight and policymaking on secret surveillance practices. Some reformers have called for abolishing or prohibiting any secret laws or interpretations that control investigations. In his 2011 speech mentioned above, Senator Wyden acknowledged that surveillance activities are necessarily secret.[58] He insisted, however, that the policies governing those activities should be debated and decided openly, through normal democratic processes. He argued that secret laws, or secretly sanctioned interpretations of laws, are incompatible with democracy.

---

56 Jennifer Granick, "NSA's Creative Interpretations of Law Subvert Congress and the Rule of Law," *Forbes* (December 16, 2013), available at http://www.forbes.com/sites/jennifergranick/2013/12/16/a-common-law-coup-detat-how-nsas-creative-interpretations-of-law-subvert-the-rule-of-law/.

57 In fact, shortly after the State of the Union address, the Office of the Director of National Intelligence announced some minor changes to surveillance practices. See Dustin Volz, "Obama Administration Announces New Rules on NSA Spying," *National Journal* (February 3, 2015).

58 *Congressional Record* 157 (May 26, 2011), S3387.

This position is appealing from the standpoint of democratic principles. But we find it too simple. There will inevitably be intelligence methods that offer major benefits for investigations and that require secrecy—even about general practices or capabilities—to be fully effective. These methods will often raise new issues of policy, or require change in existing policy; but discussing the policy openly will, in itself, reveal the methods and undermine their effectiveness. In such cases, there are only three options for Congress: forego using the new methods, despite the resulting sacrifice of investigative effectiveness; delegate the decisions about them, without legislative guidance, to the intelligence agencies; or adopt secret laws or interpretations to control their use. We believe the last option—acknowledging the need for secret policies—is the preferable course. Instead of abolishing secret laws, amendments, or interpretations, reformers should try to establish processes for making them that help minimize their frequency and provide some degree of accountability to Congress and the public.[59]

Such a process, even if achievable, would be far from fully democratic. But it would provide far more accountability to Congress and the public than do secret executive interpretations reviewed simply by the FISA Court.

To those ends, we think that Congress should attempt to negotiate with the president to adopt a mutually agreeable, committee-based prior review of secret executive amendments or interpretations of surveillance laws. The review should take place in closed proceedings of a modest-sized committee whose members have relevant interest and expertise—perhaps, for example, a select committee with members drawn from the Intelligence and Judiciary panels of both chambers.

Such a review could take different forms. In our view, the ideal would be a full-blown committee legislative veto—in which the committee would be required to vote to accept or reject a proposed secret interpretation before it would go into effect. However, because legislative-veto provisions operate under a constitutional cloud and are not ultimately enforceable in court, a plausible alternative is a report-and-wait provision.[60] Such a provision would require the

59 Congress has long passed secret appropriations to fund classified programs, such as weapons development. For discussion, see Lon J. Fuller, *The Morality of Law* (New Haven, CT: Yale University Press, 1964), pp. 91-92. For the most part, such appropriations do not seem as problematic as secret interpretations of surveillance policies.

60 To the dismay of many close observers of legislative-executive relations, the legislative veto was ruled unconstitutional in a 1983 Supreme Court decision (*INS v. Chadha*, 462 U.S. 919 [1983]). Thus such provisions are not enforceable in the federal courts. But that limitation has not ended a practice that both the legislative and executive branches sometimes find useful. The executive branch often accepts legislative veto provisions in legislation and then generally complies with any resulting vetoes—primarily because the arrangement makes it easier for Congress to permit broader grants of discretionary authority. See Louis Fisher, Legislative Vetoes After *Chadha*, Congressional Research Service, RS22132 (May 2, 2005); Walter J. Oleszek, *Congressional Procedures and the Policy Process*, 9th ed. (Thousand Oaks, CA: CQ Press, 2014), pp. 394-395. Jessica Korn argues not only that the "report-and-wait" provision is on sounder constitutional footing than the legislative veto, but that it is also nearly as effective in ensuring meaningful legislative participation. See Jessica Korn, *The Power of Separation: American Constitutionalism and the Myth of the Legislative Veto* (Princeton, NJ: Princeton University Press, 1996).

executive to present its intended action to the committee and wait for a specified period of time before implementing it; the measure should also oblige the committee to take up the proposal and render a (non-binding) approval or disapproval. Either way, the committee and each of its members would formally, though in secret, approve or disapprove the executive proposal.

Such a review is hardly guaranteed to provide strong protection for privacy interests. But unlike merely providing briefings for members, with attendance optional, the committee review would give an identified group of legislators specific responsibility to vote up or down on proposed secret policies. With direct responsibility to render judgment, they would have strong incentives to attend to the information made available to them. They could not defer to the executive, without taking responsibility for doing so, by pleading non-involvement. Such a process, even if achievable, would be far from fully democratic. But it would provide far more accountability to Congress and the public than do secret executive interpretations reviewed simply by the FISA Court.

Beyond the matter of secret policies, a second reform goal should be an institutional means to make concern for privacy a steadier, more reliable element of the policy process—so that effects on privacy are at least considered and managed, even if enhanced security is usually the top priority. To ensure that legislators have comprehensive, up-to-date analyses of surveillance programs, we believe that Congress should instruct the Government Accountability Office (GAO) to conduct ongoing investigations of the NSA and other intelligence agencies.

The executive branch has a several watchdogs that monitor surveillance practices, including the Inspectors General of the NSA and Justice Department, the President's Intelligence Advisory Board, and the Privacy and Civil Liberties Oversight Board (PCLOB). Although all serve important oversight functions, they have mandates that minimize privacy concerns or they are vulnerable to White House interference. The inspectors general are concerned about waste and fraud, among many other types of violations, while the Intelligence Advisory Board serves exclusively the president, making sure that executive orders and other directives are followed. Currently, only the PCLOB has a mission that considers and advocates for civil-liberties protections. Over the last year, it has produced several important reviews that weigh the surveillance benefits of eavesdropping programs against the privacy costs to Americans. However, prior to the Snowden leaks, both Presidents Bush and Obama let the Board sit empty for long periods, ensuring that it produced no oversight reports for most of its ten-year history.[61] A president hostile to oversight and accountability could take similar steps to undermine the Board's activities, especially once the Snowden scandals have faded.

As the investigative wing of Congress, the GAO faces no risk of presidential intrusion or obstruction, and has both the authority and know-how to conduct comprehensive intelligence oversight.[62] At

61 Garrett Hatch, Privacy and Civil Liberties Oversight Board: New Independent Agency Status, Congressional Research Service, RL34385 (August 27, 2012).

62 Patrick J. Donaldson, "Infiltrating American Intelligence: Difficulties Inherent in the Congressional Oversight of Intelligence and the Joint Committee Model," *American Intelligence Journal* 28:1 (2010), pp 13-28.

one time, in fact, it had a fully staffed office at NSA headquarters where it monitored surveillance activities on an ongoing basis.[63] To be sure, resurrecting the GAO's investigations and analysis of surveillance practices would not force policymakers or intelligence agencies to protect privacy interests. But it could ensure that legislators are made aware of the privacy considerations in all major decisions, and that at least one institutional unit seeks ways to minimize harm to those interests.

It may seem overly ambitious to call for two major institutional reforms—a legislative committee review of secret interpretations or amendments of surveillance laws and an enhanced mandate for the GAO. But preserving any semblance of traditional privacy for American citizens will be an increasingly difficult, if not impossible, challenge for the foreseeable future. Building institutions to improve the chances should be a national priority.

63 Steven Aftergood, "GAO Oversight of NSA: A Neglected Option," *Secrecy News* (January 6, 2014), available at http://blogs.fas.org/secrecy/2014/01/gao-nsa/.

Governance Studies
The Brookings Institution
1775 Massachusetts Ave., NW
Washington, DC 20036
Tel: 202.797.6090
Fax: 202.797.6144
brookings.edu/governance

Editor
Christine Jacobs
Beth Stone

Production & Layout
Beth Stone
Nick McLellan

EMAIL YOUR COMMENTS TO GSCOMMENTS@BROOKINGS.EDU