Issues in
Governance Studies

Number 60 July 2013

Institutional Failure in Surveillance Policymaking: Deliberating the Patriot Act

William Bendix and Paul J. Quirk

William Bendix is Assistant Professor of Political Science at Keene State College. His research focuses on Congress, legislative deliberation, and homeland security and civil liberties policies. He is working with Paul Quirk on a book-length study of the development of the Patriot Act.

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

EXECUTIVE SUMMARY

U.S. policymakers in the post-9/11 world face difficult choices between striving for higher levels of security and protecting civil liberties. Recent leaks about vast surveillance programs have raised fears that the government is using powerful tools to invade the privacy of millions of Americans. Because the Patriot Act provides a legal basis for this surveillance, it is widely held responsible for undermining constitutional rights.

Based on our ongoing research on the Patriot Act, we demonstrate major failures in congressional policymaking on domestic surveillance. Although Congress has generally sought to balance concerns for security and civil liberties, poorly deliberated decisions have undermined both values. In addition, Congress generally failed to provide for appropriate reviews of investigative methods. And when it finally identified problems with surveillance tools, it passively allowed the executive to develop solutions. The current controversies over domestic spying stem from the exploitation of this largely unstructured discretion by the Bush and Obama administrations.

We make recommendations for both substantive policy and institutional reforms. Congress should restrict seizures of personal records by requiring that they target specific suspects. It should set explicit legislative policies on investigators' access to phone records. And it should undertake

Congress should restrict seizures of personal records by requiring that they target specific suspects.

institutional reforms—on both the legislative and executive sides—to enhance advocacy of privacy interests, to improve monitoring and assessment of investigative activities, and to strengthen congressional participation in areas requiring secrecy.

Introduction

Dramatic intelligence leaks by National Security Agency (NSA) whistle blower Edward Snowden have revealed vast new eavesdropping by American authorities, at home and abroad. The leaks revealed blanket collection of domestic phone records, warrantless capture of emails from U.S internet companies, and wiretaps on offices of friendly foreign governments and the European Union, among other things. The revelations have triggered widespread fears of an Orwellian Big-Brother security establishment. The *Los Angeles Times* declared that Presidents George W. Bush and Barack Obama have constructed "a brave new world of pervasive surveillance."[1] The *Washington Times* asserted that the Fourth Amendment has been effectively "stripped out" of the Constitution by the executive.[2] And a Bloomberg editorial questioned whether Americans are now "living in a police state."[3]

The legal basis for much of the surveillance comes from the Patriot Act. This law has attracted controversy since its passage in 2001, and the current scandal has resurrected old concerns.[4] By many accounts, Congress, in a moment of panic after the September 11 attacks, cast aside longstanding constitutional limits on government investigators. Now the impression is that not only the openly authoritarian Bush administration but also the supposedly civil libertarian Obama administration has aggressively implemented a massively intrusive security regime.

On the basis of our ongoing research on the Patriot Act, we show that the death of American privacy rights has been greatly exaggerated. As a broad generalization, the Patriot Act has taken a balanced approach to the conflict between security and privacy. Moreover, the Obama administration has apparently maintained effective and arguably sufficient limits on governmental intrusion.

1. "Brave New World of Snooping," *Los Angeles Times* (June 7, 2013).
2. "Total Surveillance Society," *The Washington Times* (June 10, 2013).
3. "Barack Obama, Meet George Orwell," *Bloomberg View* (June 6, 2013).
4. In a recent editorial, for example, *The New York Times* called for the repeal of the Patriot Act. See "President Obama's Dragnet," *The New York Times* (June 7, 2013).

> *.... the development of Patriot Act surveillance policy has not been a pretty picture.*

Nevertheless, the development of Patriot Act surveillance policy has not been a pretty picture. Congress has ignored important information, overlooked major issues, and failed to learn from experience as it drafted, reviewed, and amended the Act. On the one hand, as liberal critics fear, it has indeed tolerated massive violations of privacy rights. On the other hand, however, it has also created pointless and costly barriers to investigations. Rather than keep working to get it right, Congress eventually, by default, passed the buck to the executive branch, where presidential administrations have developed policy solutions unilaterally and largely in secret, often expanding surveillance powers. Whatever the current state of surveillance practice, it has not been decided democratically, and it is not protected from secret, unilateral revision by future presidents.

Origins and Issues

Congress enacted the Foreign Intelligence Surveillance Act (FISA) in 1978 to place limits on domestic spying. The legislation created the FISA Court and required national-security agents for the first time to obtain judicial approval for wiretaps conducted in the United States. But over the next two decades Congress drafted a complex patchwork of surveillance laws, sometimes imposing restrictions on counterterrorism agents more severe than those facing criminal investigators.[5] The September 11 attacks gave Congress a new urgency to reexamine the FISA regime and to develop a more coherent balance between security and privacy. Congress thus drafted the Patriot Act in 2001 primarily to improve tools for fighting terrorism. But it also sought to maintain judicial oversight by reaffirming the FISA Court's jurisdiction.

Congress faced two major challenges in writing this legislation. On the one hand, the September 11 attacks made improving security—especially against potentially devastating nuclear or biological terrorism—a national priority.[6] On the other hand, there was a compelling interest in protecting traditional rights to privacy, due process, and fair trial. Ultimately, the health of American democracy was at stake. A government that can

5. For example, federal authorities could conduct roving electronic surveillance in criminal probes, but not in counter-espionage and antiterrorism cases. See Nathan C. Henderson, "The Patriot Act's Impact on the Government's Ability to Conduct Electronic Surveillance of Ongoing Domestic Communications," *Duke Law Journal* 52 (2002), pp. 179-209.

6. Graham T. Allison, *Nuclear Terrorism: The Ultimate Preventable Catastrophe* (New York: Times Books, 2004); Laurie Garrett, "The Bioterrorist Next Door," *Foreign Policy* (December 15, 2011).

investigate citizens freely—collecting and analyzing information without constraint—can use this ability to intimidate critics and suppress legitimate political opponents.

Since passing the Patriot Act, Congress has had ample opportunity to refine the legislation. In 2005, it held nearly two dozen hearings and multiple floor debates focused on the Act's most controversial surveillance provisions. Since 2006, it has held more than a dozen additional hearings and several floor votes on these same measures. House and Senate committees have heard from a broad range of witnesses—including government officials, conservative scholars, liberal activists, corporate lawyers, and spokespersons for affected ethnic and religious groups. If we tally up minutes of speeches, pages of testimony, and the like, the deliberative effort has been impressive.

Failures of Policy Deliberation

But despite the extensive proceedings, congressional debates and decisions have often been superficial and uninformed—resulting in policies that unnecessarily weakened investigations, compromised privacy rights, or both. Members of Congress, unfortunately, have few incentives to conduct thoughtful formulation of surveillance policy. They face little political risk from bolstering security at the expense of privacy, because the loss of privacy directly and immediately affects a relatively small number of people—those under investigation. In terms of electoral rewards, oversight of the executive does not compete well with legislating, let alone fundraising or speechmaking.[7] And all too often, members of Congress have greater interest in scoring partisan points or defending their party's president than in conducting careful performance evaluations. In addition to the deficient incentives, Congress has structural weaknesses that have undermined the ability to strike an intelligent, democratically sanctioned balance between security and individual rights.

Looking at how Congress developed and evaluated the Patriot Act over the last decade, we see five varieties of defective policymaking, with major consequences for the results.

1. Casual treatment of crucial provisions

To begin with, Congress has failed to give serious, careful attention to some of the most important provisions in the legislation. When the Patriot Act was first being drafted in

7. David R. Mayhew, *Congress: The Electoral Connection* (New Haven: Yale University Press, 1974); Amy Zegart and Julie Quinn, "Congressional Intelligence Oversight: The Electoral Disconnection," *Intelligence and National Security* 25:6 (2010), pp. 744-766.

the immediate aftermath of 9/11, Republicans on the House Judiciary Committee insisted that surveillance provisions include four-year sunsets, requiring reauthorization votes in 2005—an approach readily endorsed by the committee's Democratic minority.[8] Because deliberations were conducted in haste, the committee wanted the new investigative tools to be reexamined in a less turbulent atmosphere. They worried that relatively lax rules for seizing private records and conducting electronic surveillance could lead to fishing expeditions and violations of privacy rights. Instead of adopting the House approach, however, Congress acted on a Senate bill drafted in part by the Bush administration. Lawmakers placed sunsets on most, but not all, investigative provisions.[9] In fact, they overlooked perhaps the most problematic tool in the bill—national security letters—and made it permanent from the start.[10]

National security letters are a type of administrative subpoena—issued by the Federal Bureau of Investigation (FBI) on its own authority, without judicial supervision.[11] They allow investigators to seize a person's communication records, banking receipts, and credit information, without having to show evidence that the target is a spy or terrorist.[12] In effect, agents can use these letters to gather records on anyone they choose. Because the subpoenas come with no requirement to discard non-relevant information, the FBI has sometimes collected the records of innocent Americans and kept them indefinitely.[13]

In an extraordinary failure of legislative deliberation, not a single member of Congress mentioned national security letters during the floor debates in 2001. Nor did any member raise concerns about the government's prolonged retention of non-relevant information during the reauthorization debates four years later. This failure to discuss national

8. Robert O'Harrow, Jr., "Six Weeks in Autumn; A year ago, as a nation reeled from attack, a battle was joined for America's future. Not in Afghanistan. In Washington," *The Washington Post* (October 27, 2002).

9. In the House, members were uncertain about the Patriot Act because Speaker Dennis Hastert quashed the House's version and introduced the Senate's bill the morning of the floor vote. See ibid.

10. The provision authorizing national security letters appears in Title V of the Patriot Act, under "miscellaneous national security authorities." Congress only placed sunsets on provisions that appear in Title II of the Act. Likely, Congress neglected national security letters simply because they fall under a different section than all other provisions on surveillance and records seizures.

11. Specifically, they are issued by the Special Agents in Charge of FBI field offices.

12. Section 505 of the Patriot Act requires agents to stipulate that "records sought [with national security letters] are relevant to an authorized investigation to protect against international terrorism." The FBI can therefore use these subpoenas to grab the documents of people who have incidental contact with a suspect. For example, agents have obtained subpoenas on all car owners whose vehicles were parked in a hotel lot where a suspected terrorist had a room. See Eric Lichtblau, *Bush's Law: The Remaking of American Justice* (New York: Pantheon Books, 2008), pp. 92-93.

13. Charles Doyle, "National Security Letters in Foreign Intelligence Investigations: Legal Background and Recent Amendments," Congressional Research Service (September 8, 2009).

security letters was in our view the most severe deficiency in deliberations on the Patriot Act. If the Act created risks of privacy violations and fishing expeditions, it was mainly through these administrative subpoenas.

Only in late 2005, when the *Washington Post* revealed that the FBI was issuing more than 30,000 national security letters per year—"a hundredfold increase over historic norms"—did some members of Congress raise concerns.[14] Even then, many Republicans dismissed the report and showed greater interest in defending the Bush administration than in determining whether privacy violations had occurred. Eventually, an independent audit confirmed the *Post* story. Between 2003 and 2005, the FBI had issued about 140,000 national security letters and had seized private documents on almost 24,000 U.S. persons.[15] These records were added to searchable databanks, accessible to 17,000 federal agents.[16] However, by the time these findings were released in 2007, the Patriot Act had long since been reauthorized, without change in the national security letters provision. As we discuss later, although greater controls were eventually placed on the letters, Congress played almost no role in instituting the changes.

Between 2003 and 2005, the FBI had issued about 140,000 national security letters and had seized private documents on almost 24,000 U.S. persons.

2. Excessive response to organized protests

In contrast with the much-ignored national security letters, other provisions in the Patriot Act have received intense scrutiny from Congress. This scrutiny, however, has come largely in response to uninformed organized protest against expanded investigative powers. Perhaps the most scrutinized measure in the Patriot Act authorizes business-records orders. Although similar to administrative subpoenas, these orders differ in two important respects.[17] First, they enable agents to grab not only an array of sensitive files, such as financial and medical records, but also other items such as books, computers, and mobile phones. Second, these orders are issued by the FISA Court, not the FBI, and come with a statutory requirement to discard all non-relevant information.

14. Barton Gellman, "In Hunt for Terrorists, Bureau Examines Records of Ordinary Americans," *The Washington Post* (November 6, 2005).

15. U.S. Department of Justice, Office of the Inspector General, "A Review of the Federal Bureau of Investigation's Use of National Security Letters," (March 2007), pp. xvi-xxi.

16. Ibid., p. 28.

17. Section 215 of the Patriot Act.

Soon after passage of the Patriot Act, the American Library Association (ALA) became a vocal opponent of business-records orders. The group argued that the evidentiary standard for obtaining these orders was inadequate. Specifically, the orders did not require a showing of probable cause and yet allowed agents to obtain, in the view of librarians, constitutionally protected materials. Librarians worried that business-records orders would enable agents to use the reading habits of Americans to create political watch lists. Starting in 2003, the ALA organized marches against the Patriot Act with the help of several activist groups, including Amnesty International and the American Civil Liberties Union. The protests took place in several major cities and attracted the attention and broad support of the public. By the time Congress prepared to reauthorize the Patriot Act in 2005, the measure on business-records orders had aroused widespread concern and was widely discussed, incorrectly, as the "library provision."[18]

Many in Congress caved to the organized pressure. In hearings, Justice Department officials insisted that no business-records order had been used to seize data on library patrons.[19] But many lawmakers, especially Democrats, sided with the protestors. Republicans proposed special protections for libraries and bookstores. But Senate Democrats threatened to filibuster the reauthorization bill unless it also raised the evidentiary standard for all business-records orders.[20] They made this demand without seeking to establish how many business-records orders had been issued or to what extent these orders had aided terrorism investigations. In short, lawmakers failed to ask the most basic questions about the use of this investigative tool. But to avoid a filibuster, Republicans grudgingly supported the higher evidentiary standard.

In 2007, more than a year after reauthorization, an independent review of business-records orders showed that the added safeguards had been largely pointless and possibly harmful. Congress had called for the review along with the audit on national security letters. It found that the FBI had obtained only 36 business-records orders in the last five years, that it had taken investigators an average of 147 days to obtain these orders,

18. Katherine K. Coolidge, "'Baseless Hysteria': The Controversy between the Department of Justice and the Library Association over the USA Patriot Act," *Law Library Journal* 97 (2005), pp. 18-24.

19. For example, Attorney General Alberto Gonzales noted that FISA orders had been used to seize driver's license information, rental receipts, and credit card reports, but not library records. See "Oversight of the USA Patriot Act," Hearing before the Committee on the Judiciary United States Senate, 109th Congress, First Session (May 10, 2005), p. 6.

20. For a complete discussion on the evidentiary changes, see Brain T. Yeh and Charles Doyle, "USA PATRIOT Improvement and Reauthorization Act of 2005: A Legal Analysis," Congressional Research Service (December 21, 2006), pp. 5-10.

and that agents had never used them to seize library files.[21] These findings showed that Congress had acted on baseless fears about these orders. Lawmakers had accepted the unsupported complaints of activists rather than collect relevant policy information. And they had used these complaints to justify extra protections for libraries and bookstores, even though federal agents had not collected information from them.[22] Congress's failure to conduct thorough deliberations, then, led to needless policy adjustments that enhanced neither security nor privacy.

3. Neglect of learning

Although Congress authorized multiple, complex surveillance tools in the Patriot Act, it failed to mandate periodic reviews of these tools. Without regular, detailed reports on the use of surveillance measures, Congress's ability to assess national-security policy depended on the executive branch to collect systematic data and share it with legislators. This approach assumed that the FBI would compile accurate files on its activities, including any legal errors or privacy violations it may have committed. Equally problematic, it assumed that the White House would not withhold information from Congress. When lawmakers finally asked pertinent questions—such as "How many national security letters has the FBI issued?" or "How long does it take to get a business-records order?"—they could not obtain reliable answers. And without good answers, members of Congress were unable to determine whether the Patriot Act had led to abuses, facilitated the capture of terrorists, or both. As a result, legislators were unable to suggest appropriate amendments to legislation, even several years after the bill's passage.

Moreover, while Democrats were eager to investigate privacy violations under the Bush administration, they lacked the same zeal for audits once President Obama took office.

As noted before, Congress in 2006 ordered independent audits of national security letters and business-records requests. But it only did so after the *Washington Post* revealed fishing expeditions by the FBI. Moreover, while Democrats were eager to investigate privacy violations under the Bush administration, they lacked the same zeal for audits once President

21. One business-records request took authorities 604 days to process. See U.S. Department of Justice, Office of the Inspector General, "A Review of the FBI's Use of Section 215 Orders for Business Records in 2006," (March 2008).

22. The reauthorization of the Patriot Act stipulated that agents would need the personal approval of a high-level official, such as the director of the FBI, to seize library or book records. This approval would be in addition to the court requirements already in place. See Section 106 of the USA PATRIOT Improvement and Reauthorization Act of 2005.

Obama took office. In 2009, they allowed the auditing requirement for national security letters and business-records orders to expire.[23] Partisan interests clearly trumped information gathering and rigorous oversight.

4. Delegation by default

After audits belatedly revealed significant problems with both national security letters and business-records orders, Congress made little effort to improve the Patriot Act. Instead, it essentially looked away and allowed the executive to rewrite the rules for seizing private information.

Many legislators agreed that the FBI should be required to discard captured materials not linked to terrorism suspects or foreign spies. In 2007 and again in 2009, Democrats offered multiple bills that added this requirement to national security letters.[24] However, even though Democrats had large majorities in Congress, they allowed these bills to die in committee and instead deferred to the Obama administration. Eventually, Justice Department officials drafted rules requiring agents to delete all non-relevant information gathered with national security letters.[25] It is unclear why Congress passed the buck to the Obama administration. But by doing so, it gave the executive the latitude to loosen or eliminate these rules at some later point.

Congress also failed to revisit the business-records provision. Initially, it appeared that lawmakers were willing to ignore security concerns and let six-month processing delays of court orders hamper investigations. However, recent leaks about NSA programs indicate that Congress had in effect simply turned the entire issue over for secret policymaking by the executive branch.

Recently, *The Guardian* reported that the Bush administration in 2006, without public disclosure, had adopted a radical reinterpretation of the business-records provision to authorize the daily collection of all domestic phone records.[26] These data, or "metadata" as they are termed, include the phone numbers of callers and receivers, the length and

23. Michelle Richardson, "National Security Letters: A Note on Numbers," ACLU (May, 12, 2012), http://www.aclu.org/blog/national-security/national-security-letters-note-numbers.

24. See, for example, The National Security Letters Reform Act of 2007 (H.R. 3189, S. 2088) and the JUSTICE Act of 2009 (H.R. 4005, S. 1686).

25. Charles Doyle, "National Security Letters: Proposals in the 112th Congress," Congressional Research Service (February 1, 2011), pp. 16-17.

26. Glen Greenwald, "Revealed: NSA Collecting Phone Records of Millions of Americans Daily," *The Guardian* (June 5, 2013).

time of calls, and sometimes the locations of phone participants. Originally, the business-records provision granted far more limited authority. It allowed investigators to capture private materials on the basis of a court order in a specified terrorism case.[27] The Bush administration decided that such an order could be used to capture all communication logs from a specific phone carrier, such as Verizon or AT&T. Authorities could now scoop up tens of millions of phone records with a single order issued by the FISA Court.

The Bush administration first briefed members of Congress about the metadata program in 2006.[28] Yet aside from two senators, Mark Udall (D-CO) and Ron Wyden (D-OR), no one objected to the NSA dragnet or the drastic modifications to the business-records provision.[29] By letting Bush's reinterpretation (subsequently maintained by Obama) go unchallenged, Congress abdicated its legislative role and allowed the executive to develop new surveillance law unilaterally.

5. Ineffective participation in matters requiring secrecy

As often occurs in national-security policy, Congress had difficulty exerting influence on issues that demanded secrecy. If all 535 members routinely participated in classified discussions, damaging leaks might be almost constant. Instead, Congress normally settles for limited briefings, typically including only members of the Intelligence committees. On especially sensitive matters, briefings have been limited to eight congressional leaders.[30] This system has preserved secrecy but often at the expense of genuine congressional participation. With only four members from each party privy to critical information, legislators will rarely resist the administration position on a major issue.

As recent reports on the metadata program show, Congress has struggled to conduct effective oversight of domestic spying.[31] Although Congress received briefings, many

27. One of the drafters of the Patriot Act pointed out the change in the scope of surveillance: "Congress intended to allow the intelligence communities to access targeted information for specific investigations. How can every call that every American makes or receives be relevant to a specific investigation?" See Jim Sensenbrenner, "This Abuse of the Patriot Act Must End," *The Guardian* (June 9, 2013).

28. Leslie Cauley, "NSA Has Massive Database of Americans' Phone Calls," *USA Today* (May 10, 2006).

29. Since at least 2011, Senators Udall and Wyden have noted their objections to the classified interpretation of the Patriot Act in letters sent to colleagues and the Justice Department.

30. The so-called Gang of Eight include the leaders in the House and Senate, as well as the chairs and ranking members of the Intelligence committees. See Denis McDonough, Mara Rudman, and Peter Rundlet, "No Mere Oversight: Congressional Oversight of Intelligence Is Broken," Center for American Progress (June 2006), p. 22.

31. This problem is hardly new. In 2004, the 9/11 Commission reported that congressional scrutiny of the Intelligence Community was "dysfunctional." See U.S. National Commission on Terrorist Attacks upon the United States, *The 9/11 Commission Report: Final Report* (Washington: GPO, 2004), p. 420.

lawmakers only learned of the program when *The Guardian* ran its stories. Members on the Intelligence committees received the bulk of the briefings, and provided opportunities for their colleagues in the House and Senate to view top-secret files. But many skipped the sessions because classified briefings were seen as pointless. Lawmakers could not take notes, consult experts, or discuss technical matters with staff, thus limiting their ability to assess classified information.[32]

These restrictions did not apply to members on the Intelligence committees, who were uniquely able to follow the metadata program. But the Intelligence panels lacked a hands-on familiarity with the legal issues concerning both records seizures and the FISA Court procedures, because the Judiciary committees had done most of the work on the Patriot Act. But even if the Intelligence panels had sufficient legal understanding, they were confined to discuss policy in a classified setting and therefore were in no position to mobilize Congress against a presidential program that few members knew about or understood.

Outcomes and Controversies

Because of the recent leaks, major surveillance programs conducted by the NSA are now enmeshed in controversy. To a great extent, public concerns stem from the deficient deliberations and oversight that Congress has performed on surveillance policy over the last decade. Some criticism appears to exaggerate the threats to privacy interests that the programs pose. But it does not inspire public confidence when most lawmakers are as surprised by news of government spying as the constituents they represent. At a minimum, Congress has not adequately addressed important policy issues or conducted sufficient oversight.

... it does not inspire public confidence when most lawmakers are as surprised by news of government spying as the constituents they represent.

The first leak revealed the metadata program. Authorized by Bush and continued by Obama, the program allows the government to collect all domestic phone records. Despite its broad scope, there appears to be some need for this bulk seizure of records. Because telecom carriers eventually destroy billing information, authorities collect and

32. Tim Starks, "Intelligence Oversight Split on Access between Haves, Have-Notes," *Congressional Quarterly/Roll Call* (June 10, 2013); Jonathan Weisman, "White House Says Congress Was Briefed 13 Times on Surveillance Programs," *The New York Times* (June 8, 2013).

store their communication logs to permit later access to records of actual suspects.[33] According to available reports, the NSA does not review or share captured data; agents must obtain separate approval from the FISA Court to examine the phone records of a specified target.[34] The Obama administration has insisted that this surveillance is narrowly focused, claiming that authorities examined the records of fewer than 300 individuals in 2012.[35]

The second recent leak exposed the PRISM program.[36] Under PRISM, the NSA captures foreign communications—such as emails, video chats, and file transfers—that pass through U.S. servers. From the standpoint of American privacy interests, this surveillance may not be objectionable. Because the communications are initiated overseas, the NSA does not need a court order to intercept the conversations. Rather, the attorney general and the director of national intelligence jointly approve surveillance on suspects located outside the United States. Agents then present the joint order, or "directive," to the internet company (such as Google or Yahoo), and obtain the emails of foreign customers identified in the request. The FISA Court is briefed on this surveillance to ensure that authorities do not intercept U.S. communications in the process.[37] While PRISM is not part of the Patriot Act, it is authorized by related, follow-up legislation, the FISA Amendments Act of 2008. [38]

According to publicly available information, both the metadata and PRISM programs include safeguards designed to protect against privacy violations and warrantless eavesdropping by government agents. For the safeguards to work effectively, however, Congress needs to conduct consistent oversight of both the Intelligence Community and

33. Statement of Rep. Mike Rogers (R-MI), *This Week with George Stephanopoulos*, ABC (June 9, 2013).

34. James Ball, "NSA Data Surveillance: How Much Is Too Much?" *The Guardian* (June 10, 2013).

35. Ellen Nakashima, "Call Records of Fewer than 300 People Were Searched in 2012, U.S. Says," *The Washington Post* (June 15, 2013).

36. Barton Gellman and Laura Poitras, "U.S., British Intelligence Mining Data from Nine U.S. Internet Companies in Broad Secret Program," *The Washington Post* (June 6, 2013); Glen Greenwald and Ewen MacAskill, "NSA Taps in to Internet Giants' Systems to Mine User Data, Secret Files Reveal," *The Guardian* (June 6, 2013).

37. Glenn Greenwald and James Ball, "The Top Secret Rules that Allow NSA to Use US Data without a Warrant," *The Guardian* (June 20, 2013). See also Ryan Gallagher, "Fact and Fiction in the NSA Surveillance Scandal," *Slate* (June 26 2013); Edward C. Liu, "Reauthorization of the FISA Amendments Act," Congressional Research Service (April 8, 2013).

38. PRISM replaced the Terrorist Surveillance Program. In 2001, President Bush had approved the Terrorist Surveillance Program to give the NSA authority to capture international communications of U.S. persons without court approval. Bush ended the program in 2007 because of controversy. Congress passed the FISA Amendments Act to give the NSA limited authority to capture international communications that pass through the United States.

the FISA Court. Yet it has a track record of delegating duties to the executive, valuing secrecy over deliberation, and relying heavily on a few lawmakers to understand and follow the actual uses of powerful surveillance tools. Congress, as it operates now, lacks the ability to identify—let alone stop—serious investigative abuses when and if they occur.

Recommendations

...we have reason to believe that other important surveillance operations remain classified and undisclosed.

It is debatable whether the U.S. government, overall, has struck a defensible balance between enhancing security and protecting civil liberties. We have seen the implementation of expansive surveillance programs, and we have reason to believe that other important surveillance operations remain classified and undisclosed.[39] It is even possible that the executive has withheld eavesdropping activities from Congress. But if recent accounts by Intelligence members are accurate, we have also seen that agents follow multiple court procedures—first by seeking judicial approval to seize records and then by obtaining separate, highly targeted approval to examine records. Most of the very few members of Congress who have closely monitored the FISA process believe that it includes reasonable safeguards. Still, the policymaking system has been overly secretive, dominated by the executive, and slow to identify gaps in privacy protections. We suggest both changes to the Patriot Act and, more important, changes to the institutional arrangements for making decisions on surveillance policy.

The most obvious and immediate need is to place permanent restrictions on national security letters. Congress should pass legislation mandating that authorities discard all non-relevant information captured with administrative subpoenas. The Obama administration has already implemented this policy through a Justice Department directive. But until it becomes a statutory requirement, either the current or a succeeding administration could easily cancel this safeguard and allow agents, as they did in the Bush administration, to stockpile personal information of innocent Americans. Since this reform merely codifies current practice, a permanent safeguard would protect privacy without creating new investigative obstacles.

39. After attending a recent briefing, Rep. Loretta Sanchez (D-CA) described the Snowden leaks as "just the tip of the iceberg." See Glenn Greenwald, "On Prism, Partisanship and Propaganda," *The Guardian* (June 14, 2013). The little-known UPSTREAM program apparently allows the NSA to access fiber-optic cables directly in order to capture international phone and email communications that pass through the U.S. See also James Bamford, "They Know Much More Than You Think," *The New York Review of Books* (August 15, 2013).

Congress also needs to revisit the business-records provision. The executive now uses business-records orders in a much broader way than Congress intended, collecting all domestic phone data with blanket FISA requests. We think that Congress should quash such a radical departure from the legislative intent and reaffirm that a business-records order may only be used in a particular investigation with named suspects. Six weeks after the Snowden leaks, the House, by a 205-217 vote that divided both parties, defeated a measure that went even further—not only restoring the limitations on business-records orders, but explicitly ending the metadata program.

We are undecided whether the bulk collection of phone records should continue under new provisions. Available information on NSA activities remains sketchy, making it difficult to evaluate either the investigative effectiveness or the privacy costs of metadata collection. Congress needs to conduct a thorough investigation of this program. If it concludes that bulk data collection is vital to security needs, it should pass authorizing legislation with strong privacy protections. For example, rather than allowing the NSA to stockpile metadata for possible future, targeted use, Congress could require phone companies to keep the information for longer periods and compensate them for it. If Congress finds the metadata collection unnecessary or overly intrusive, it should pass legislation directly barring it. One way or the other, Congress should reclaim policymaking authority over the collection of phone records.

To improve congressional deliberations on surveillance policy, we suggest that Congress constitute a new, expanded, and strengthened select committee to receive briefings on domestic surveillance policy. It should consist of selected members from several committees, including the Judiciary committees, and not just the Intelligence panels. Without including multiple committees and at least a dozen or so members from each House, Congress cannot marshal sufficient expertise or generate sufficient consensus or authority to control the executive on critical security matters. To minimize the risk of leaks, the participating legislators could undergo the same security clearances and exposure to investigation and potential sanctions as top executive-branch security officials.[40] The select committee should be empowered to deliberate in secret and make legislative recommendations to the president or the full Congress.

...we suggest that Congress establish a radically enhanced, independent office of privacy.

40. Congress has considered a number of similar proposals. See Frederick M. Kaiser, "Protection of Classified Information by Congress: Practices and Proposals," Congressional Research Service (August 31, 2011).

Finally, we suggest that Congress establish a radically enhanced, independent office of privacy. Although a modest Office of Privacy and Civil Liberties currently exists in the Department of Justice, it reports to the attorney general. An effective watchdog would either report to Congress, like the Government Accountability Office or the Congressional Budget Office, or else operate independently within the executive branch, as with the Inspectors General. Crucially, it should have full security clearances and a legislative mandate to monitor surveillance activities, evaluate their results from a privacy standpoint, investigate possible rights violations, perform regular audits and special studies, and advocate for privacy interests at the FISA Court, in congressional hearings, and in other venues.

These are ambitious institutional reforms. But as surveillance technologies become ever more sophisticated, and potential terrorist attacks increasingly devastating, to maintain a healthy balance between security and privacy will depend on overcoming the institutional weaknesses in policy deliberation that have been demonstrated over the unedifying twelve-year history of the Patriot Act. To overcome those weaknesses within the constitutional framework of American government will require institution-building on both the legislative and executive sides.

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

Editing
Christine Jacobs

Production & Layout
Beth Stone
Emma Goldberg

Email your comments to gscomments@brookings.edu