Center for American Progress

Adapting to the Future of Intelligence Gathering

By Peter Juul July 23, 2013

When the Soviet Union shot down a U-2 reconnaissance aircraft on a mission in the airspace over its country in 1960, President Dwight D. Eisenhower justified the spy mission on the grounds that, "No one wants another Pearl Harbor."[1] Policymakers today face a similar imperative: preventing another 9/11. With that goal in mind, they have authorized or otherwise presided over a massive expansion of the size, capabilities, and authorities of America's intelligence community.

The recent rediscovery that the National Security Agency, or NSA, collects, stores, and analyzes vast amounts of data from the global telecommunications network raises important questions about the wide-ranging post-9/11 activities of America's intelligence community. These questions have surfaced amid the emergence of a suite of online tools that enable both the government and private entities to track and predict individuals' behavior. This raises broader questions about the nature and future of online privacy in a world where both public and private actors have access to increasingly sophisticated and personalized information on individuals. The collection of personal data—whether for national-security or private purposes and especially in a new era of information technology that is marked by the rise of social media—poses critical questions about the role of government, the physical protection of the country, and the rights to individual privacy guaranteed by law and the Constitution.

Recent news stories on various NSA programs illustrate the increasingly close relationships between information-technology, or IT, companies on one hand and U.S. intelligence agencies such as the NSA on the other.[2] These companies—as well as telecommunications corporations—already collect large amounts of personal data from their users, in large part through social-media use, online shopping, and web browsing and searching. This data is, in turn, passed to the NSA and other U.S. intelligence agencies under orders from the Foreign Intelligence Surveillance Court, or FISC, through mechanisms such as PRISM,[3] which appears to be a secure data-storage device where companies can deposit information subpoenaed for the NSA via the FBI.[4] In short, the NSA and other intelligence agencies are obtaining personal data in bulk from private corporations that already collect it everyday.

The proliferation of personal-data collection by private companies is a cornerstone of the NSA programs highlighted in recent reports. Verizon—the telecommunications company named in the widely discussed leaked FISC order requiring that the company turn over customer "metadata" to the government—has been selling that same metadata to private clients such as the Phoenix Suns basketball team since at least October 2012.[5] "Just as NSA officials say the agency uses data on Americans only to hunt for terrorists and spy on foreign adversaries," *Los Angeles Times* reporter Ken Dilanian writes, "Silicon Valley executives say they use personal information only to sell advertising and improve the customer experience."[6] The NSA's data collection is, in fact, considered less revealing and more legally restricted than the private data collection that businesses and others employ.

The renewed interest in NSA activities has raised a series of broader and more complex questions about online privacy, the role of private contractors in the U.S. security sector, and oversight of the activities of the NSA and America's other intelligence agencies. By their very nature, these questions move beyond the specifics of the various NSA programs that have been reported on in recent weeks. They have been left largely unanswered as technology has advanced, and safeguarding the country from terrorism has grown ever more important as both a political and policy imperative over the past decade plus.

In this issue brief, we discuss our nation's need to update online privacy laws and address the privatization of intelligence gathering that was previously a public-sector duty, as well as ways to balance national security with the legal and constitutional rights of Americans.

We need clear, updated rules for online privacy

Recently reported NSA programs rest on a foundation of personal data collected by private corporations. This data collection is often justified by recourse to lengthy terms-of-use agreements that are unintelligible to the average customer, most of whom simply click "agree" to access their desired program or service.

But it can also be intrusive. Target, for instance, created an algorithm to predict when female customers were pregnant based on their purchases and then recommend pregnancy and other baby-related products to these women.[7] Smartphones with built-in GPS services can be used as tracking devices. Facebook is well known for giving users' private information to advertisers,[8] and Google's ill-fated Buzz social-networking service violated users' privacy[9] to such an extent that Google was forced to settle with the Federal Trade Commission, or FTC, over privacy violations and deceptive practices.[10] Netflix used its customers' viewing habits to determine its first round of original programming, including shows such as "House of Cards" and "Arrested Development,"[11] while Amazon's Prime service plans to do the same. Amazon already uses an algorithm to track users' buying and browsing habits and recommend items for purchase from its online store.[12]

Accepting terms-and-conditions agreements allows companies to mine personal user data

Many popular applications, programs, and services require users to sign off on lengthy legal terms-of-service conditions before they are able to use them. Apple's terms and conditions for its popular iTunes music store alone run more than 5,300 words.[13] Amazon's terms and conditions run comparatively shorter at more than 3,400 words,[14] while Netflix's terms of use are more than 9,000 words.[15] By comparison, the maximum word count for a professional journal such as *The New England Journal of Medicine* is 3,000 words,[16] while the "appropriate" word count for an academic journal such as *International Security* is 10,000 words to 15,000 words.[17] Many users understandably do not read these terms and conditions in close detail, instead simply clicking that they agree to them in order to use the application or service right away.

Moreover, these terms-of-use conditions often obscure the way in which users agree to forfeit their privacy when agreeing to use the services in question. Google,[18] Netflix,[19] Amazon,[20] and Apple[21] bury their privacy policies in links within their terms-of-use and service agreements. Privacy policies for all four of these companies run higher than 2,200 words, creating an additional burden for users. These privacy policies tell users who dare attempt to read them that the companies providing the services they want to use will collect vast amounts of their personal information. Netflix, for instance, collects information:

> *[I]ncluding but not limited to: your online activity, title selections, reviews, ratings, payment history, correspondence, Internet protocol addresses, device types, unique device data (such as device identifiers), operating systems, instant watching of movies, TV shows and related activity. We use this information for such purposes as determining your general geographic location, providing localized content, enforcing our terms (such as using device identifiers to determine your eligibility for a free trial), providing recommendations on movies & TV shows we think will be enjoyable, personalizing the service to better reflect particular interests, tracking your instant-watching hours, determining your Internet service provider, helping us quickly and efficiently respond to inquiries and requests and otherwise enhancing or administering our service offering for you and other users. We also provide analysis of our users in the aggregate or otherwise in anonymous form to prospective partners, advertisers and other third parties. We may also disclose and otherwise use, on an anonymous basis, movie & TV show ratings, consumption habits, commentary, reviews and other information. For example, we use movie & TV show ratings and consumption behavior to improve our recommendations to you as well as other users.*[22]

Google, Amazon, and Apple privacy policies all contain similar, if somewhat less detailed, information on how they collect users' personal information.

What's more, these privacy policies also make clear that these companies disclose the personal information they collect to third parties. Some of these disclosures can be benign or helpful, such as Apple's provided example of exchanging information with a cell-phone provider to activate a newly purchased iPhone. But the information sharing allowed by privacy polices often goes beyond what is necessary to help products such as iPhones function. Apple, for instance:

> *[S]hares personal information with companies who provide services [to Apple] such as information processing, extending credit, fulfilling customer orders, delivering products to you, managing and enhancing customer data, providing customer service, assessing your interest in our products and services, and conducting customer research or satisfaction surveys.*[23]

Netflix and Amazon have similar statements in their privacy policies, while Google's policy is less specific.

Notably, the privacy policies of all four companies examined here contain statements to the effect that the companies will share information with governments to, in Google's words, "meet any applicable law, regulation, legal process or enforceable governmental request."[24] Apple's privacy policy similarly states that it "may also disclose information about you if we determine that for purposes of national security, law enforcement, or other issues of public importance, disclosure is necessary or appropriate." This disclosure, Apple's privacy policy says, may occur "by law, legal process, litigation, and/or requests from public and governmental authorities within or outside your country of residence."[25]

In effect, users have agreed that the personal information they provide to these companies will be available to the legal requests of any government, such as a warrant issued by the Foreign Intelligence Surveillance Court under the USA PATRIOT Act and the FISA Amendments Act.

This private collection of personal data has been occurring with less public debate than the congressional authorization of expanded government surveillance powers. By forcing users to agree to these terms-of-use contracts prior to accessing a service, private companies are obtaining permission to collect and mine personal data, as well as permission to give that data to the government if they deem it necessary. This points to a need to update online privacy laws and norms to take into account new forms of personal-information collection that have been developed just since the turn of the millennium. Current online privacy law rests on the 1986 Electronic Communications Privacy Act, or ECPA, and subsequent adjustments such as the USA PATRIOT Act of 2001 and FISA Amendments Act of 2008 that expanded government surveillance powers.[26]

While there has been little action to update these laws, several proposals have been offered for bringing online privacy regulations up to date. In 2012 the FTC issued a report on protecting consumer privacy online based on a series of "fundamental principles,"[27] and the Obama administration has called for an online "consumer privacy bill of rights."[28] More recently, Sens. Patrick Leahy (D-VT) and Mike Lee (R-UT) proposed updating the ECPA to reflect technological changes and advances.[29] These proposals should be studied seriously, and ultimately, their broader common goal of an updated online privacy framework covering both the government and private entities should be enacted in some form after careful consideration.

We must ensure inherently governmental intelligence functions remain in public hands

According to a 2010 investigation by *The Washington Post*, the U.S. government contracted 1,931 private companies to work on counterterrorism, homeland security, and intelligence programs across the country in that year alone. Of the more than 854,000 people with top-secret security clearances, 265,000 were private contractors.[30] One-third of the CIA's workforce—10,000 positions—is composed of private contractors, while the NSA contracts with at least 484 companies. According to a 2008 study commissioned by the Office of the Director of National Intelligence, private contractors made up 29 percent of the intelligence community's workforce at a cost equivalent to half of the intelligence community's personnel budget.[31] That is, private-contractor workers cost significantly more than public-sector workers but do not count against the intelligence community's personnel budgets.

Private contractors and government intelligence

The role of Edward Snowden, a private contractor working for Booz Allen Hamilton, in disclosing sensitive NSA programs raises deep and troubling questions over the outsourcing of inherently governmental functions related to surveillance and national security. As a March 2009 memo issued by President Barack Obama noted:

> *[T]he line between inherently governmental activities that should not be outsourced and commercial activities that may be subject to private sector competition has been blurred and inadequately defined. As a result, contractors may be performing inherently governmental functions.*[32]

The U.S. government currently defines inherently governmental functions according to the Federal Activities Inventory Reform Act of 1998 as those functions that are "so intimately related to the public interest as to require performance by Federal Government employees."[33] In response to President Obama's 2009 memo, the Office of Federal Procurement Policy issued guidelines in 2011 to help federal agencies determine which of their functions are inherently governmental. Among these guidelines was a requirement for agencies to identify "critical functions" so as "to ensure they have sufficient internal capability to maintain control over functions that are core to the agency's missions and operations."[34]

It appears clear that the NSA has been outsourcing critical, inherently governmental functions to private contractors in the years of explosive intelligence growth that followed 9/11. According to James Bamford, a longtime reporter on the agency, NSA contracts rose from 55 in October 2001 to 7,197 in October 2005, and contracting companies grew from 144 to 4,388.[35] As part of its hearings into the privatization of the intelligence community, Congress should ensure that agencies such as the NSA identify their critical, inherently governmental functions and give them appropriate resources to ensure government employees, not private contractors, perform these functions.

In addition to the potential for unauthorized disclosure of sensitive information by poorly vetted contractors—as appears to have been the case with Edward Snowden[36]—the proliferation and penetration of private contractors into the U.S. intelligence community raises more consequential issues. These contactors have financial incentives to further increase the size of the intelligence community itself and their role within it, without reference to the effectiveness or even legality of their performance. Even more, the prevalence of contractors raises questions about the inherently governmental nature of the tasks they are contracted to perform and whether we should allow private workers to do what should be done by public-sector employees. Finally, the privatization of the U.S. intelligence community poses a major challenge to transparency, oversight, and informed consent of its activities.

Congress should conduct a full range of hearings to investigate and review these questions and other challenges posed by the privatization of the intelligence community. It should also recommend strategic and operational changes to the current system. Other questions to be answered include the data to which contractors have access, the relationship between contractors and other private firms—particularly telecommunications and IT firms—and the overall financial and nonfinancial costs of contracting out the functions of America's intelligence agencies.

We should reform oversight to balance national-security actions with legal protections

New institutional mechanisms should be put in place at the NSA and other relevant government agencies to bolster oversight and predict the future legal, ethical, and social implications of developments in telecommunications, computing, and surveillance capabilities.

First and foremost, the basic mechanisms surrounding the Foreign Intelligence Surveillance Court should be reworked to offer more robust internal oversight of its operations. Legal and intelligence community "red teams" with proper clearances and access to information could be established within the Justice Department, the NSA, and other relevant agencies to challenge FISA warrant requests when appropriate or necessary.

Moreover, oversight of the FISC itself should be broadened beyond the appointment and supervision of its members, which is currently done by the chief justice of the Supreme Court. Justice Department officials and members of Congress from relevant committees could also be involved in the appointment and supervision of the FISC, ensuring representation from the elected executive and legislative branches of government.

The NSA, along with other government agencies, should set aside time, money, and personnel to consider the legal, ethical, and social implications of the technologies they develop or otherwise rely on to conduct their work. The mass shift to fiber-optic cables as the primary means to transmit data at the turn of the millennium, for example, created problems with existing surveillance law. Anticipating developments such as this and fully debating their implications should be a priority for relevant government agencies. While a fully accurate prediction is impossible, attempting to sketch out likely future developments and how they will impact society, norms, and laws can help produce better responses to technological evolution than hasty, secret actions and post-facto public responses.

Internal units dedicated to assessing the implications of advances in data collection and analysis could serve as pilot projects for other similar units dedicated to assessing technological advances in general. Autonomous weapons systems, nanotechnology, cyber espionage and cyber warfare, neuroscience, and other areas are advancing rapidly without coherent thought given to the policy, legal, and ethical implications of these advances. Preparing for these advances will be crucial.

We should establish a national commission to examine these issues in full

The actions proposed for the three issues above will not fully address the complex set of issues raised by the reports of NSA surveillance. A more thorough top-to-bottom look at online privacy, government surveillance, and the role of private contractors in intelligence in the age of ever-advancing information and telecommunications technology should be undertaken. President Obama should issue an executive order forming a national commission on the future of online privacy to more thoroughly address the issues outlined in this brief.

Presidential commissions have been used to address serious issues ranging from the Pearl Harbor and 9/11 attacks to defense reform and aviation security. Most recently, President Obama established the Presidential Commission on Election Administration.[37] The recommendations of these commissions have often led to legislation—the Packard Commission informing the Goldwater-Nichols Act that reformed the Defense Department and U.S. military, for instance[38]—and can complement independent congressional efforts.

A presidential commission examining current online privacy matters—including NSA surveillance activities and the laws governing them—should include privacy, technology, and legal experts, as well as distinguished Americans from the national-security community and Congress. Its mission should be wide ranging, examining existing laws governing online privacy and surveillance such as the ECPA, the USA PATRIOT ACT, and the FISA Amendments Act, among others. It should also look into the current state of telecommunications and information technology and their likely future evolution. Its remit should not be restricted to government activities but should extend to private-sector activities such as those described earlier in this issue brief. The commission should also examine the existing governance of the intelligence community under the FISC, as well as the implications of the intelligence community's increasing reliance on private contractors.

The commission should be charged with formulating actionable recommendations that protect both the freedoms guaranteed to Americans by law and the Constitution, as well as the physical security of the country. These recommendations should attempt to anticipate future technological developments in order to provide a flexible framework in which to accommodate them.

Conclusion

Recent reporting on NSA surveillance has created an opportunity for a broader discussion of online privacy, the privatization of the intelligence community, and ways to better prepare for technological advances and social change in the future. These questions should not be lost amid examinations of particular NSA programs—nor should they be subsumed in abstract treatises on the balance between liberty and security. While the philosophical issues raised are important, they are better addressed in substantive discussions of the concrete issues outlined here.

Over the past decade the U.S. government and many American companies have plowed ahead on data collection and analysis while expanding private contracting of inherently governmental functions. The time has come to have full and complete deliberation of these issues.

Peter Juul is a Policy Analyst with the National Security and International Policy team at the Center for American Progress.

Endnotes

1 "Dwight D. Eisenhower, 1953-61." In Center for the Study of Intelligence, ed., Our First Line of Defense: Presidential Reflections on US Intelligence (Washington: Central Intelligence Agency 2008), available at https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/books-and-monographs/our-first-line-of-defense-presidential-reflections-on-us-intelligence/eisenhower.html.

2 James Risen and Nick Wingfield, "Web's Reach Binds N.S.A. and Silicon Valley Leaders," The New York Times, June 19, 2013, available at http://www.nytimes.com/2013/06/20/technology/silicon-valley-and-spy-agency-bound-by-strengthening-web.html.

3 "NSA slides explain the PRISM data-collection program," The Washington Post, July 10, 2013, available at http://www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/.

4 Kurt Eichenwald, "PRISM Isn't Data Mining and Other Falsehoods in the N.S.A. 'Scandal'," Vanity Fair, June 14, 2013, available at http://www.vanityfair.com/online/eichenwald/2013/06/prism-isnt-data-mining-NSA-scandal.

5 Anton Troianovski, "Phone Firms Sell Data on Customers," The Wall Street Journal, May 21, 2013, available at http://online.wsj.com/article/SB10001424127887323463704578497153556847658.html.

6 Ken Dilanian, "The NSA is watching. So are Google and Facebook," Los Angeles Times, June 30, 2013, available at http://www.latimes.com/news/nationworld/nation/la-na-consumer-tracking-20130701,0,3719521.story.

7 Charles Duhigg, "How Companies Learn Your Secrets," The New York Times, February 16, 2012, available at http://www.nytimes.com/2012/02/19/magazine/shopping-habits.html.

8 Michael Daly, "You Thought You Had Privacy Before the NSA Leak? What About Facebook?", The Daily Beast, June 13, 2013, available at http://www.thedailybeast.com/articles/2013/06/13/you-thought-you-had-privacy-before-the-nsa-leak-what-about-facebook.html.

9 Molly Wood, "Google Buzz: Privacy Nightmare," CNET News, February 10, 2010, available at http://news.cnet.com/8301-31322_3-10451428-256.html.

10 Federal Trade Commission, "FTC Gives Final Approval to Settlement with Google over Buzz Rollout," October 24, 2011, available at http://ftc.gov/opa/2011/10/buzz.shtm.

11 David Carr, "Giving Viewers What They Want," The New York Times, February 24, 2013, available at http://www.nytimes.com/2013/02/25/business/media/for-house-of-cards-using-big-data-to-guarantee-its-popularity.html.

12 JP Mangalindan, "Amazon's recommendation secret," CNNMoney, July 30, 2012, available at http://tech.fortune.cnn.com/2012/07/30/amazon-5/.

13 Apple, "iTunes Store - Terms and Conditions," available at http://www.apple.com/legal/internet-services/itunes/us/terms.html (last accessed July 2013).

14 Amazon, "Conditions of Use," available at http://www.amazon.com/gp/help/customer/display.html/?nodeId=508088 (last accessed July 2013).

15 Netflix, "Terms of Use," available at https://signup.netflix.com/TermsOfUse (last accessed July 2013).

16 The New England Journal of Medicine, "Frequently Asked Questions: About Manuscript Submissions," available at http://www.nejm.org/page/author-center/frequently-asked-questions#submissions (last accessed July 2013).

17 MIT Press Journals, "International Security: Submission Guidelines," available at http://www.mitpressjournals.org/page/sub/isec (last accessed July 2013).

18 Google, "Privacy Policy," available at http://www.google.com/intl/en/policies/privacy/ (last accessed July 2013).

19 Netflix, "Privacy Policy," available at https://signup.netflix.com/PrivacyPolicy (last accessed July 2013).

20 Amazon, "Amazon.com Privacy Notice," available at http://www.amazon.com/gp/help/customer/display.html/ref=hp_left_sib?ie=UTF8&nodeId=468496 (last accessed July 2013).

21 Apple, "Privacy Policy," available at https://www.apple.com/privacy/ (last accessed July 2013).

22 Netflix, "Privacy Policy."

23 Apple, "Privacy Policy."

24 Google, "Privacy Policy."

25 Apple, "Privacy Policy."

26 Charles Doyle, "Privacy: An Overview of the Electronic Communications Privacy Act" (Washington: Congressional Research Service, 2012), available at http://www.fas.org/sgp/crs/misc/R41733.pdf.

27 Federal Trade Commission, "Protecting Consumer Privacy in an Era of Rapid Change" (2012), available at http://ftc.gov/os/2012/03/120326privacyreport.pdf.

28 The White House, "Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy" (2012), available at http://www.whitehouse.gov/sites/default/files/privacy-final.pdf.

29 Office of Sen. Patrick Leahy, "Leahy, Lee Introduce Legislation to Update Electronic Communications Privacy Act," Press release, March 19, 2013, available at http://www.leahy.senate.gov/press/leahy-lee-introduce-legislation-to-update-electronic-communications-privacy-act.

30 Dana Priest and William M. Arkin, "A hidden world, growing beyond control," The Washington Post, July 19, 2010, available at http://projects.washingtonpost.com/top-secret-america/articles/a-hidden-world-growing-beyond-control/.

31 Dana Priest and William M. Arkin, "National Security Inc.," The Washington Post, July 20, 2010, available at http://projects.washingtonpost.com/top-secret-america/articles/national-security-inc/print/.

32 Office of the Press Secretary, "Memorandum for the Heads of Executive Departments and Agencies – Subject: Government Contracting," Press release, March 4, 2009, available at http://www.whitehouse.gov/the_press_office/Memorandum-for-the-Heads-of-Executive-Departments-and-Agencies-Subject-Government/.

33 Federal Activities Inventory Act of 1998, Public Law 105-270, 105th Cong., 2d sess. (October 19, 1998), available at http://www.whitehouse.gov/omb/procurement_fairact.

34 Office of Management and Budget, "Policy Letter 11-01, Performance of Inherently Governmental and Critical Functions," Federal Register 76 (176) (2011): 56227–56242, available at http://www.gpo.gov/fdsys/pkg/FR-2011-09-12/pdf/2011-23165.pdf.

35 James Bamford, The Shadow Factory: The Ultra-Secret NSA from 9/11 to the Eavesdropping on America (New York: Anchor, 2008).

36 Lindsay Wise, "Contractor responsible for Snowden's security clearance investigated for inadequate background checks," McClatchy, June 20, 2013, available at http://www.mcclatchydc.com/2013/06/20/194556/contractor-responsible-for-snowdens.html.

37 Pam Fessler, "Obama Forms Presidential Commission to Study Voting Problems," NPR, March 28, 2013, available at http://www.npr.org/blogs/itsallpolitics/2013/03/28/175605639/obama-forms-presidential-commission-to-study-voting-problems.

38 Charles Nemfakos and others, "The Perfect Storm: The Goldwater-Nichols Act and Its Effect on Navy Acquisition" (Washington: RAND Corporation, 2010), available at http://www.rand.org/content/dam/rand/pubs/occasional_papers/2010/RAND_OP308.pdf.