E
N
G
A
G
E

A Federalist Society Symposium on the National Security Agency's Bulk Data Seizures and FISA Surveillance Programs

Presented by the International & National Security Law Practice Group

Contributions from:

Randy E. Barnett & Jim Harper

Steven G. Bradbury

Jeremy Rabkin

Stewart A. Baker

Nathan A. Sales

Jameel Jaffer & Laura W. Murphy

Robert F. Turner

Grover Joseph Rees

October 2013

International & National Security Law

A Federalist Society Symposium on the National Security Agency's Bulk Data Seizures and FISA Surveillance Programs

Contributions from Randy E. Barnett & Jim Harper, Steven G. Bradbury, Jeremy Rabkin, Stewart A. Baker, Nathan A. Sales, Jameel Jaffer & Laura W. Murphy, Robert F. Turner, & Grover Joseph Rees

Note from the Editor:

We are pleased to bring you this special *Engage* Symposium on the National Security Agency's bulk data seizures and Foreign Intelligence Surveillance Act programs. This Symposium features diverging points of view on the issues involved from top scholars and experts in the field. As always, the Federalist Society takes no position on particular legal or public policy initiatives. All expressions of opinion are those of the authors. Additionally, we invite responses from our audience. To join this debate, please email us at info@fed-soc.org.

Why NSA's Bulk Data Seizures Are Illegal and Unconstitutional

Randy E. Barnett & Jim Harper***

Introduction

The National Security Agency's ("NSA") data collection program, designed and built to collect information about every American's telephone calls, stands on weak statutory footing and raises grave concerns under the Fourth and Fifth Amendments. If Congress does not revisit these programs, the courts should invalidate them.

I. The NSA Data Collection Program is Inconsistent with the Plain Meaning of the Statute and Congressional Intent Passing It

Section 215 of the USA-PATRIOT Act[1] allows Foreign Intelligence and Surveillance Act judges ("FISA") to issue orders requiring the production of tangible things upon satisfactory application by the FBI. The statutory language[2] requires an investigation in existence at the time such a judge issues a Section 215 order. Because the NSA's Section 215 orders do not pertain to an existing investigation, they are not authorized by the statute.

Section (b) of 50 U.S.C. § 1861 specifies that an application for a Section 215 order must include "a statement of facts showing that there are reasonable grounds to believe that the tangible things sought are relevant to an authorized investigation . . . ."[3] In two ways, this language requires an investigation to pre-exist any such application.

First, the required statement of facts must show that the things sought "*are* relevant"[4] to an investigation. It thus requires a showing *at the time of application* that the things sought are relevant to an investigation. This standard presumes and requires the existence of an investigation in progress at the time of application.

Second, the statement of facts required by 50 U.S.C. § 1861(b)(2)(A) must show that the application is relevant to an "authorized" investigation. It is impossible to determine that an investigation is or will be "authorized" if the investigation has not come into existence. Therefore, a FISA judge cannot properly conclude that a *future* investigation, including investigations arising from analyzing the seized data, met the standards of the statute.

Because the NSA's Section 215 orders do not pertain to existing authorized investigations, they violate the plain language of the statute. In passing Section 215, Congress did not intend to create authority for collection of information beyond that which is relevant to an existing investigation. Report language accompanying a precursor of Section 215, clarifies Congress's purposes:

> The Administration had sought administrative subpoena authority without having to go to court. Instead, section 156 amends title 50 U.S.C. § 1861 by providing for an application to the FISA court for an order directing the production of tangible items such as books, records, papers, documents and other items upon certification to the court that the records sought are *relevant to an ongoing foreign intelligence investigation*.[5]

By its choice of language, Congress did not intend to allow applications with merely *potential* relevance to foreign intelligence generally. Instead it intended to restrict them to existing, discrete, "ongoing" investigations, not applications for general surveillance.

II. The NSA's Section 215 Bulk Data Collection Orders are Unconstitutional

A. Blanket Data Seizures Are Modern Day General Warrants

The Fourth Amendment has two parts: First, "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated."[6] And second, "no warrants shall issue, but upon

---

**Carmack Waterhouse Professor of Legal Theory, Georgetown University Law Center; Director, Georgetown Center for the Constitution.* *This essay was adapted from the Brief for Cato Institute as Amcius Curiae Supporting Petitioner, In re: Electronic Privacy Information Center, No. 13-58 (U.S. Aug. 12, 2013). We thank Jason Kestecher and Elizabeth Gusfa for their research assis-tance.*

***Director of Information Policy Studies, Cato Institute.*

probable cause, supported by oath or affirmation, and *particularly describing the place to be searched, and the persons or things to be seized*."[7] The Fourth Amendment was adopted to prevent general or nonspecific warrants.

The Fourth Amendment requires the things to be searched or seized under a warrant to be described "particularly."[8] But the order issued to Verizon under the NSA data collection program requires the company to produce "on an ongoing daily basis … all call detail records."[9] Because they are not "particular," such orders are the modern incarnation of the "general warrants" issued by the Crown to authorize searches of American colonists. As with general warrants, blanket seizure programs subject the private papers of innocent people to the risk of searches and exposure, without their knowledge and with no realistic prospect of a remedy.

The Founders thought that the seizure of "papers" for later perusal or "searching" was an abuse distinct from, but equivalent to, the use of general search warrants, which is why "papers" was included in the Fourth Amendment in addition to "effects" or personal property.[10]

> [A]t the heart of Whig opposition to seizing papers was the belief that any search of papers, even for a specific criminal item, was a general search. It followed that any warrant to sift through documents is a general warrant, even if it is specific to the location of the trove and the item to be seized.[11]

Allowing blanket seizures of privately-held data would constitute an unprecedented legal and constitutional sea change that should be undertaken, if at all, only after robust public debate and a constitutional amendment that is itself worded specifically enough to govern the executive branch in the future. It is not a policy that should emerge from an advisory panel of judges to which the People are not privy.

B. Property and Contract Define When a Seizure Requires a Warrant

For good reason, the Fourth Amendment uses a possessive pronoun—"their"—to describe the "persons, houses, papers, and effects" it protects.[12] People's ownership of themselves and their things is an essential counterweight to state power. The Fourth Amendment has long and appropriately been administered with reference to property. Two terms ago, in *United States v. Jones*,[13] the Supreme Court held that the "reasonable expectation of privacy" formulation from *Katz v. United States*[14] does not supplant, but adds protection beyond the protection of one's property from unreasonable searches and seizures. "[T]he *Katz* reasonable-expectation-of-privacy test," wrote Justice Scalia, "has been added to, not substituted for, the common-law trespassory test."[15]

While *Katz* has become the lodestar in current Fourth Amendment jurisprudence, the "reasonable expectations" language that now dominates the academic literature and case law actually appears, not in the majority opinion of the Court, but in a solo-concurrence by Justice Harlan. Harlan's formulation has proven to be a weak rule for deciding cases. As Justice Alito observed in *Jones*, the "*Katz* expectation-of-privacy test . . . involves a degree of circularity, and judges are apt to confuse their own expectations of privacy with those of the hypothetical reasonable person to which the *Katz* test looks."[16] In addition, "the *Katz* test rests on the assumption that this hypothetical reasonable person has a well-developed and stable set of privacy expectations."[17]

The "reasonable expectation of privacy" test reverses the inquiry required by the Fourth Amendment. Justice Stewart's majority opinion in *Katz* properly rested on the physical protection that the defendant had given to his oral communications. "What a person *knowingly exposes to the public*, even in his own home or office, is not a subject of Fourth Amendment protection. But what he *seeks to preserve as private*, even in an area accessible to the public, may be constitutionally protected."[18] What Katz

> sought to exclude when he entered the booth was not the intruding eye—it was the uninvited ear. He did not shed his right to do so simply because he made his calls from a place where he might be seen. No less than an individual in a business office, in a friend's apartment, or in a taxicab, a person in a telephone booth may rely upon the protection of the Fourth Amendment. One who occupies it, shuts the door behind him, and pays the toll that permits him to place a call is surely *entitled to assume* that the words he utters into the mouthpiece will not be broadcast to the world.[19]

Rather than airy and untethered speculations about "reasonable expectations," the courts should return to the traditional—and more readily administrable—property and contract rights focus of Fourth Amendment protection reflected in the majority opinion in *Katz*. Courts should examine how parallels to the walls of the home and the phone booth in *Katz* conceal digital information are employed by the people to preserve their privacy.

An inquiry into the physical and legal barriers people have placed around their information — for example, by using passwords to restrict access to their email, or entering into terms of service agreements that include privacy protections — can generally answer whether they have held it close. This establishes the threshold of personal security that the Fourth Amendment requires a warrant to cross. No distinction should be made between sealing a letter before handing it to the postman, taking a phone call in a secluded phone booth, password-protecting one's email, or selecting a communications company with a suitable privacy policy.

In short, the physical and legal barriers people place around their information define both their actual and "reasonable" expectations of privacy and should provide the doctrinal touchstone of the search warrant requirement. When one has arranged one's affairs using physics and the law of property and contract to conceal information from preying eyes, government agents may not use surreptitious means and outré technologies like thermal imaging[20] to defeat those arrangements without obtaining a warrant that conforms to the requirement of the Fourth Amendment. In *Jones*, the Court took an important step in this direction. It should now recognize the privacy of informational data that has *in fact*, in the words of the Fourth Amendment, been "secure[d]" by sufficient physical and legal

protections.

With this in mind, the Court should either adapt the third-party doctrine to modern circumstances or reject it altogether. *Smith v. Maryland*,[21] which upheld the use of pen registers without a warrant, was a classic "reasonable expectation of privacy" case, and a paragon of its maladministration. Common experience shows that phone companies keep phone data private from everyone but the customer and a small circle of service providers that are bound to the phone companies' privacy rules. The public "reasonably expects" these records are kept from government agencies absent a warrant and consents to disclose this information to phone companies on that condition.

Some members of the Supreme Court have already recognized *Smith*'s poor reasoning and its irreconcilability with the Information Age. As Justice Sotomayor noted in *Jones*, the third-party doctrine "is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks."[22]

With the NSA's program of "pen registers for everyone," yesterday's tomorrow has already arrived. *Smith v. Maryland* and a third-party doctrine permitting blanket seizures of data that has been disclosed to a third party under contractual and regulatory restrictions is patently inapt for the age of mass storage of data accessed in secret by super computers.

III. The FISA Court is Inconsistent with the Due Process of Law

The procedures established by the Foreign Intelligence Surveillance Act do not provide communications companies and their customers the "due process of law" required by the Fifth Amendment. In contrast to the typical adjudication of a search warrant's validity, the constitutionality of a massive program of data seizure is being adjudicated in secret. No targeted customer has the right to intervene and contest the case, nor even to read the decision purporting to uphold the constitutionality of the seizure of its data.

In the seminal case on the role of federal courts, the Supreme Court ruled: "A case or controversy, in order that the judicial power of the United States may be exercised thereon, implies the existence of present or possible adverse parties whose contentions are submitted to the court for adjudication."[23] The absence of a genuine "case or controvery" means that the FISA Court is not a genuine Article III court, but is instead simply a part of the executive branch. The deprivation of property by such a court in secret proceedings justified by secret orders and constitutional rulings is the antithesis of the Due Process of Law guaranteed by the Fifth Amendment.

Conclusion

In a republican form of government based on popular sovereignty, the people are the principals or masters and those in government are their agents or servants. For the people to control their servants, they must know what their servants are doing. The secrecy of these programs, and the proceedings by which their constitutionality is assessed, make it impossible to hold elected officials and appointed bureaucrats accountable. Internal governmental checks, and even secret congressional oversight, are no substitute for the sovereign people being the ultimate judge of their servants' conduct in office.

Such judgment and control is impossible without the information that secret programs conceal. Without the recent leaks, the American public would have no idea of the existence of these programs, and it still cannot be certain of their scope. What we do know reveals that these programs are contrary to statute, and unconstitutional under any theory. The American people need relief from this unprecedented surveillance of them by their servants.

Endnotes

1 Pub. L. No. 107-56, 115 Stat. 272.

2 50 U.S.C. § 1861.

3 50 U.S.C. § 1861(b)(2)(A).

4 *Id.*

5 H.R. Rep. No. 107-236, pt. 1, at 61 (2001) (emphasis in original).

6 U.S. Const. amend. IV.

7 *Id.* (emphasis added).

8 *Id.*

9 *In re:* Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things from (FISC) (Docket No. BR 13-80) (April 25, 2013), at 3.

10 *See generally* Donald A. Dripps, *Dearest Property: Digital Evidence and the History of Private "Papers" as Special Objects of Search and Seizure,* 103 J. Crim. L. & Criminology 49 (2013) (explaining how the seizure of papers to be later searched for evidence of criminality was considered to be a distinct but equally disturbing abuse than that of general warrants to search houses).

11 *Id.* at 104.

12 U.S. Const. amend. IV.

13 132 S. Ct. 945 (2012).

14 Katz v. United States, 389 U.S. 347 (1967).

15 *Jones*, 132 S. Ct. at 952. *See also id.* at 954-55, (Sotomayor, J. concurring) ("Of course, the Fourth Amendment is not concerned only with trespassory intrusions on property. Rather, even in the absence of a trespass, a Fourth Amendment search occurs when the government violates a subjective expectation of privacy that society recognizes as reasonable." (quotations and citations omitted)).

16 *Id.* at 962 (Alito, J. concurring) (citations omitted).

17 *Id.*

18 *Katz*, 389 U.S. at 351 (emphasis added).

19 *Id.* at 352 (emphasis added).

20 *See* Kyllo v. United States, 533 U.S. 27 (2001).

21 Smith v. Maryland, 442 U.S. 735 (1979).

22 *Jones*, 132 S. Ct. at 957 (Sotomayor, J., concurring) (citation omitted).

23 Muskrat v. United States, 219 U.S. 346 (1911) (citing Chisholm v. Georgia, 2 U.S. (2 Dall.) 431 (1793)).

Before the House Committee on the Judiciary

Oversight Hearing into the Administration's Use of FISA Authorities

July 17, 2013

*Steven G. Bradbury**

Thank you, Chairman Goodlatte, Ranking Member Conyers, and distinguished Members of the Committee. I appreciate the opportunity to appear before the Committee today to address the statutory authorities and constitutional principles governing the two National Security Agency programs that have been the subject of recent disclosures. These are:

- First, the acquisition of telephone call-detail records that involves only telephone metadata, not the content of any phone calls or the names or addresses of any phone subscribers.
- Second, the surveillance, including the so-called "PRISM" Internet collection, that is targeted at the communications of foreign persons reasonably believed to be located outside the United States.

I believe it is most useful to discuss the legal basis for each of these two programs separately, since they are authorized under two different provisions of the Foreign Intelligence Surveillance Act, or FISA, though of course the programs can and should work together as part of the overall counterterrorism efforts of the United States.

I. Section 215 Order for Acquisition of Telephone Metadata

Let me focus first on the telephone metadata program. As the government has stated, this program is supported by a business records order issued under the provision of FISA added by Section 215 of the USA PATRIOT Act.[1] This Section 215 order must be reviewed and reapproved by the federal judges who sit on the FISA court every 90 days. I understand that fourteen different federal judges have approved this order since 2006.

The metadata acquired consists of the transactional information that phone companies retain in their systems for a period of time in the ordinary course of business for billing purposes and that appears on typical phone bills. It includes only data fields showing which phone numbers called which numbers and the time and duration of the calls. *This order does not give the government access to any information about the content of calls or any other subscriber information, and it doesn't enable the government to listen to anyone's phone calls.*

Access to the data is limited under the terms of the court order. Contrary to some news reports, there's no data mining or random sifting of the data permitted. The database may only be accessed through queries of individual phone numbers and only when the government has reasonable suspicion that the number is associated with a foreign terrorist organization. If it appears to be a U.S. number, the suspicion cannot be based solely on activities protected by the First Amendment, such as statements of opinion, books or magazines read, Web sites visited, or places of worship frequented. Any query of the database requires approval from a small circle of designated NSA officers.

A query will simply return a list of any numbers the suspicious number has called and any numbers that have called it and when those calls occurred. Nothing more.

The database includes metadata going back five years, to enable an analysis of historical connections. Any records older than five years are continually purged from the system and deleted.

In analyzing links to suspicious numbers, any connections that are found to numbers inside the United States will of course be of most interest, because the analysis may suggest the presence of a terrorist cell in the U.S. Based in part on that information, the FBI may seek a separate FISA order for surveillance of a U.S. number, but that surveillance would have to be supported by individualized probable cause.

The NSA has confirmed that in all of 2012, there were fewer than 300 queries of the database, and only a tiny fraction of the data has ever been reviewed by analysts. The database is kept segregated and is not accessed for any other purpose, and FISA requires the government to follow procedures overseen by the court to minimize any unnecessary dissemination of U.S. numbers generated from the queries.

In addition to court approval, the 215 order is also subject to oversight by the executive branch and Congress. FISA mandates periodic audits by inspectors general and reporting to the Intelligence and Judiciary Committees of Congress. When Section 215 was reauthorized in 2011, I understand the leaders of Congress and members of these Committees were briefed on this program, and all members of Congress were offered the opportunity for a similar briefing.

II. Legal Basis and Constitutional Standards

Now let me address the statutory and constitutional standards applicable to the acquisition of this telephone metadata.

Section 215 permits the acquisition of business records that are "relevant to an authorized investigation." Here, the telephone metadata is "relevant" to counterterrorism investigations because the use of the database is essential to conduct the link analysis of terrorist phone numbers described above, and this type of analysis is a critical building block in these investigations. In order to "connect the dots," we need the broadest set of telephone metadata we can assemble, and that's what this program enables.

The legal standard of relevance in Section 215 is the same standard used in other contexts. It does not require a separate showing that every individual record in the database is "relevant" to the investigation; the standard is satisfied if the use of the

Steven G. Bradbury is a Partner at Dechert LLP in Washington, DC. Previously Mr. Bradbury served as head of the Office of Legal Counsel at the Department of Justice, where he was principal deputy assistant attorney general from 2004-2009 and acting assistant attorney general from 2005-2007.

database as a whole is relevant. As I've indicated, the acquisition of this data and the creation and use of this database are not only relevant to ongoing counterterrorism investigations; they're necessary to those investigations, because they offer the only means to conduct the critical analysis that provides links to new phone numbers used by agents of foreign terrorist organizations.

In terms of the background constitutional principles, it's important to remember that the Fourth Amendment itself would not require a search warrant or other individualized court order for such data acquisition. A government request for a company's business records is not a "search" within the meaning of the Fourth Amendment. Government agencies have authority under many federal statutes to issue administrative subpoenas without court approval for documents that are "relevant" to an authorized inquiry. In addition, grand juries have broad authority to subpoena records potentially relevant to whether a crime has occurred, and grand jury subpoenas also don't require court approval. In the modern world of electronic storage and data compilation, reliance on the same "relevance" standard in these other contexts can also result in extremely expansive requests for business records.

In addition, the Fourth Amendment does not require a warrant when the government seeks purely transactional information, or metadata, as distinct from the content of communications. This information is voluntarily made available to the phone company to complete the call and for billing purposes, and courts have therefore said there's no reasonable expectation that it's private.[2]

I would stress, however, that Section 215 is more restrictive than the Constitution demands, because it requires the approval of a federal judge. In this way, Congress in the PATRIOT Act adopted a requirement for judicial review and approval of FISA business records orders that is more protective of privacy and civil liberties interests than the Constitution would otherwise demand. And while the 215 order for metadata is extraordinary in terms of the amount of data acquired, it's also extraordinarily narrow and focused in terms of the strict limitations placed on accessing the data at the back end.

III. Section 702 Order Targeting Foreign Communications

Let me now turn to the other NSA program at issue: The surveillance program targeting the Internet and other communications of foreign persons reasonably believed to be outside the United States. This program, which includes the so-called "PRISM" collection, is supported by a FISA court order issued under Section 702 of FISA, the provision for "programmatic" foreign-targeting authority that was added by the FISA Amendments Act of 2008.[3] Similar authority was initially provided on a temporary basis in the Protect America Act of 2007.

The best way to understand this foreign-targeting program is to review the provisions of Section 702, which lays out the governing framework approved by Congress.

Section 702 provides that the Attorney General and the Director of National Intelligence may jointly authorize, for up to one year at a time, targeted surveillance of the communications of non-U.S. persons who are reasonably believed to be located outside the United States to acquire foreign intelligence information, provided the FISA court approves the targeting procedures under which the surveillance occurs and the minimization procedures that govern use of the acquired information.

Under Section 702, the surveillance may not (1) intentionally target any person, of any nationality, known to be located in the United States, (2) target a person outside the U.S. if the purpose is to reverse target any particular person believed to be in the U.S., (3) intentionally target a U.S. person anywhere in the world, and (4) intentionally acquire any communication as to which the sender and all recipients are known to be in the U.S.

Section 702 requires the Attorney General to adopt, and the FISA court to approve, targeting procedures reasonably designed to ensure compliance with these limitations, as well as detailed minimization procedures designed to ensure that any information about U.S. persons captured through this surveillance will not be retained or disseminated except as necessary for foreign intelligence reporting purposes.

Any foreign intelligence surveillance that is targeted at a particular U.S. person or any person believed to be in the United States requires a traditional individualized FISA order supported by probable cause.

Like the business records provision of FISA, Section 702 goes beyond the baseline protections of the Fourth Amendment. Federal courts have consistently held that the Constitution permits the executive branch to conduct intelligence surveillance within the United States without court involvement, provided the surveillance is focused on foreign threats.[4] By establishing a detailed procedure for court approval and congressional oversight, Section 702 therefore provides a system of foreign intelligence surveillance that is more restrictive than the Constitution would otherwise require.

The PRISM Internet collection is precisely the type of court-approved foreign-targeted intelligence surveillance that Congress intended to authorize when it enacted and reauthorized Section 702 by overwhelming majorities. This program is subject to extensive reviews and periodic reports to Congress by inspectors general, in addition to the oversight of the FISA judges. Moreover, I understand that in advance of the reauthorization of Section 702 in 2012, the leaders and full membership of the Intelligence Committees of both Houses of Congress were briefed on the classified details of this program and all members of Congress were offered the opportunity for such a briefing.

* * *

For these reasons, I think these two programs are entirely lawful and are conducted in a manner that appropriately respects the privacy and civil liberties of Americans and the principles enshrined in the Constitution. Thank you, Mr. Chairman.

Endnotes

1 *See* 50 U.S.C. § 1861.

2 *See* Smith v. Maryland, 442 U.S. 735, 743-44 (1979); Quon v. Arch Wireless Operating Co., 529 F.3d 892, 904-05 (9th Cir. 2008).

3 *See* 50 U.S.C. § 1881a.

4 *See, e.g.*, United States v. Truong Dinh Hung, 629 F.2d 908, 914 (4th Cir. 1980).

NSA is in Trouble for Good Reason

*Jeremy Rabkin**

The surveillance programs conducted by the National Security Agency are in trouble. The fundamental reason is that the American people no longer have confidence that data collected by the government will be used solely for national security purposes. Abstract legal arguments won't restore public trust, because the distrust is not grounded in abstract concerns about executive power or the precise application of the Fourth Amendment. The prevailing atmosphere of distrust will be hard to dispel because, given what has emerged in the past two years, distrust is an entirely reasonable response.

The scale of public suspicion was dramatized by the vote in the House of Representatives on July 24, where the so-called Amash-Conyors Amendment, prohibiting the NSA from conducting data-mining of phone call records, failed by only a dozen votes. A resounding majority of Democrats (111-83) voted for the Amendment – flaunting their suspicion of a program defended (and conducted) by a president of their own party. The NSA's longstanding surveillance authority was saved by Republican votes in the House. But even Republicans, traditionally the party of strong measures for national security, were notably divided: more than 40% of Republican House members (94 of 228) defied the calls of their party leaders and endorsed proposed restrictions on the NSA.

An extensive survey by the Pew Research Center (released on July 26) confirmed that the House vote reflected a larger shift in public opinion. Indeed, it understated the scale of the shift. It found that a near majority of Americans (47%) now worries that efforts to detect terror threats have become a threat to civil liberties, while notably fewer (35%) now think these efforts do not go far enough to protect against terrorism. A similar poll in October 2010 found only 32% worried about threats to civil liberties against 47% who worried that monitoring of terror threats did not go far enough. So there has been a swing of opinion by 15 percentage points in public opinion on the programs in less than three years. Overall, the swing of opinion among Republican voters was 18 percentage points—leaving them now as likely as Democrats to worry about threats to civil liberties from U.S. government surveillance over threats from terror attacks from inadequate intelligence. The swing among Republicans identifying with the Tea Party was nearly twice that—a 35 percentage point swing (from 20% worrying about surveillance threats to civil liberties in 2010 to 55% in July 2013).

People do, after all, have reason to be distrustful—based on information in the public record. The first thing that has become widely known is that, whatever secret information the government may collect, it does a very poor job at keeping secrets. Edward Snowden triggered the current debate by releasing information about NSA programs. Some of what was publicized in his name may already have been known, some of what was reported might have been misleading or distorted. But if the government has not denied the truth of his claims about spying on U.N. meetings and various meetings of foreign governments. How did Snowden gain access to these secrets as a low level contract employee? Why was somebody of limited skill and no proven loyalty given access to these secrets? How was he able to down-load masses of information from government computers without being detected, before he fled to China and then Russia with his secrets?

What makes the whole episode more remarkable is that it came a full three years after Army Private Bradley Manning was arrested for forwarding troves of secret diplomatic correspondence to WikiLeaks. Somehow the United States government had arranged a security system in which an army private was given access to a vast array of classified documents of no relevance to his own responsibilities—and no one noticed that he was using government computers to gain access, over an extended period, to these documents. The consequences were not trivial: by revealing secret diplomatic reports, he put world leaders on notice that nothing they say to American diplomats can be kept confidential. That will surely be a burden on American diplomacy for years to come. A military judge ultimately sentenced Manning to 35 years in prison, even though he was acquitted of charges that he had deliberately set out to aid America's enemies.

But for all the evident harm caused by these leaks, the government seems to have done no serious review of how they occurred. At his sentencing, Manning's lawyers revealed that he was a very troubled young man who had confided to military superiors that he wanted a sex change operation. Was an army private with severe psychological problems really a safe person to trust with sensitive secret materials? How was it that no one thought about whether to give such a person access to the whole range of American diplomatic correspondence? How was it that after the uproar resulting from the leaks, no one was fired, no one even thought to ask probing questions of the Secretary of State or the Secretary of Defense?

Secretary of Defense Robert Gates did protest – in bitter language ("Shut the F—up!")—when White House officials started boasting to the press about details of the raid that had killed Osama bin Ladin in May of 2011. There was some protest about extensive reports, published in *The New York Times* in June of 2012, revealing details of the STUXNET computer virus, deployed by the CIA against the Iranian nuclear program. The administration promised to stop the leaks and punish the leakers. No one has been charged, let alone punished—even though it seems clear, given accounts in both stories about what the President himself said in intimate meetings, that some of the information could only have come from a small circle of suspects.

Add it all up and there is a very clear pattern: The government is not serious about keeping its own secrets, so why believe it would be careful with other people's secrets? And

Jeremy Rabkin is a Professor of Law at George Mason University. He serves on the Board of Directors of the U.S. Institute of Peace (originally appointed by President George W. Bush in 2007, then appointed for a second term by President Barack Obama and reconfirmed by the Senate in 2011).

if information gleaned from surveillance is not confined to those using it for proper national security purposes, it may be deployed for improper purposes. Is that far-fetched? It's a nearly irresistible suspicion.

In March of 2012, a gay rights advocacy group published the tax return of the National Organization for Marriage ("NOM"), an organization opposing gay marriage. Included were the names of donors to NOM. Someone in the IRS leaked the document. Other conservative organizations also had their tax filings leaked. Perhaps the leaks were perpetrated by rogue agents, like Bradley Manning or Edward Snowden. That would still be worrisome—since they haven't been identified and indicted, more than a year later.

But we can't be at all confident that such abuses of the IRS simply reflected the initiative of low-level operatives. That was the initial explanation for the IRS policy of delaying approval for Tea Party groups seeking tax exempt status before the 2012 elections and that story has since been refuted by new revelations of directives from IRS officials in Washington. White House promises to "get to the bottom" of IRS abuses have so far gone nowhere. It has not, it seems, been a priority to stop them. Officials even at higher levels must be aware that Barrack Obama's career has been boosted in the past by leaks of information supposed to be confidential. Most notably, Obama's path to the Senate in 2004 was greatly smoothed by the mysterious (still unexplained and unpunished) release of sealed court records relating to the divorce proceedings of Jim Ryan, forcing the strongest potential Republican candidate to drop out of the race. Officials in the Obama administration do not seem to know there is anything wrong with revealing secrets, when that serves the immediate political needs of the top man.

So, no surprise that conservative groups now distrust the NSA. Former Vice President Cheney admonished, in an August appearance, "the NSA is different from the IRS." It's true that continuing revelations about the scale of NSA surveillance have not yet indicated anything that looks like partisan abuse. But what has come out is that the Director of National Intelligence, James Clapper, lied to Congress when he testified in March of 2013 that the NSA did not collect individual communications of American citizens. We have learned that the NSA has collected tens of thousands of individual email messages and phone messages, including a great many involving American citizens in the United States. We have also learned that the FISA court—in previously secret rulings—rebuked the government for misrepresenting its programs when seeking authorization for new surveillance undertakings. And everything we have learned comes from submissions which NSA, itself, has chosen to release. We do not know what more abuses it may still be concealing.

So there is much reason for concern. But there is also much reason to worry about terror threats and much reason to think that NSA surveillance can be extremely helpful in detecting and thereby helping to deflect threats from terrorists. The most alarming finding of the PEW poll is that 70% of Americans believe NSA data collection is not restricted to national security efforts but "also used for other purposes." And one of the most telling findings is that even among those who believe this, 43% still support the program (against 53% seeking restrictions). You can worry about NSA abuses—and still conclude we need to have the NSA exercising vigorous surveillance.

The President has proposed adjustments in the procedure for authorizing NSA surveillance, including provision for an outside advocate to challenge government requests before the FISA court. I do not see how anything useful can be achieved by tinkering with the authorization procedures. They will still remain secret and therefore one-sided, at least from the point of view of actual targets of the surveillance.

The focus should be not so much on limiting what information government can collect but on limiting the way it uses that information. It's one thing to have government know what numbers you call (or what email addresses you contact or what websites you frequent) and something else to have the government leak this information to people with other agendas than national security. For the proper purpose, people will share very confidential information with doctors or lawyers which they wouldn't want others to know.

The main recourse has to be government self-correction: those who are found to be leaking information should be punished—severely and in public. It is already a crime for government employees to release confidential information (18 U.S.C. §1905). Congress has thought it proper to underline the point in special situations—as with release of financial records by any "farm credit examiner" (18 U.S.C. §1907). We might enact a new statute to encourage and facilitate relevant prosecutions, emphasizing the special offense of improperly circulating national security data damaging to American citizens. Vigorous, exemplary prosecutions might help to restore public trust.

But given the Obama administration's flagrant public assertions of a general authority to decline to enforce existing laws —declaring broad-ranging dispensations from immigration law and its own health care law—it will be hard to reassure people that such abuses will actually be punished. Therefore, we ought to consider giving victims of national security leaks a private right of action to sue officials who are responsible for release of personal, confidential information shown to be damaging to the plaintiff. We might also specify liability for reckless management of such confidential information, by higher officials who did not personally circulate such information but failed to take precautions against abuse by their subordinates.

There are obvious objections. Lawsuits of this kind might expose honest officials to harassing litigation. Concerns about personal liability might inhibit officials from sharing intelligence information within the government, even for proper purposes. A workable statute would have to define the liability in ways that might limit such unwelcome effects. It may be that, after closer consideration, Congress will conclude that there is indeed no safe way to impose personal liability for such bureaucratic abuse in an area where officials must constantly make sensitive, disputable decisions about what information should be shared and with whom.

But anyone who wants to save the NSA must focus on reassuring the public that information collected for national security purposes will only be used for national security pur-

poses. The Obama administration has not exerted much effort to provide that reassurance. It is not clear it does want to save the program, which its own core constituencies do not support. But we won't save the NSA by measures that provide just enough gesture toward reform to deflect blame from the Obama White House for mounting public suspicions.

Oversight Hearing on FISA Surveillance Programs

Committee on the Judiciary

United States Senate

July 31, 2013

*Stewart A. Baker**

Mr. Chairman, Ranking Member Grassley, members of the Committee, it is an honor to testify before you on such a vitally important topic. The testimony that I give today will reflect my decades of experience in the areas of intelligence, law, and national security. I have practiced national security law as general counsel to the National Security Agency, as general counsel to the Robb-Silberman commission that assessed U.S. intelligence capabilities and failures on weapons of mass destruction, as assistant secretary for policy at the Department of Homeland Security, and in the private practice of law.

To be blunt, one of the reasons I'm here is that I fear we may repeat some of the mistakes we made as a country in the years before September 11, 2001. In those years, a Democratic President serving his second term seemed to inspire deepening suspicion of government and a rebirth of enthusiasm for civil liberties not just on the left but also on the right. The Cato Institute criticized the Clinton administration's support of warrantless national security searches and expanded government wiretap authority as "dereliction of duty," saying,"[i]f constitutional report cards were handed out to presidents, Bill Clinton would certainly receive an F—an appalling grade for any president—let alone a former professor of constitutional law."[1] The criticism rubbed off on the FISA Court, whose chief judge felt obliged to give public interviews and speeches defending against the claim that the court was rubber-stamping the Clinton administration's intercept requests.[2]

This is where I should insert a joke about the movie "Groundhog Day." But I don't feel like joking, because I know how this movie ends. Faced with civil liberties criticism all across the ideological spectrum, the FISA Court imposed aggressive new civil liberties restrictions on government's use of FISA information. As part of its "minimization procedures" for FISA taps, the court required a "wall" between law enforcement and intelligence. And by early 2001, it was enforcing that wall with unprecedented fervor. That was when the court's chief judge harshly disciplined an FBI supervisor for not strictly observing the wall and demanded an investigation that seemed to put the well-regarded agent at risk of a perjury prosecution. A chorus of civil liberties critics and a determined FISA Court was sending the FBI a single clear message: the wall must be observed at all costs.

And so, when a law enforcement task force of the FBI found out in August of 2001 that al Qaeda had sent two dangerous operatives to the United States, it did . . . nothing. It was told to stand down; it could not go looking for the two al Qaeda operatives because it was on the wrong side of the wall. I believe that FBI task force would have found the hijackers—who weren't hiding—and that the attacks could have been stopped if not for a combination of bad judgment by the FISA Court (whose minimization rules were later thrown out on appeal) and a climate in which national security concerns were discounted by civil liberties advocates on both sides of the aisle.

I realize that this story is not widely told, perhaps because it's not an especially welcome story, not in the mainstream media and not on the Internet. But it is true; the parts of my book that describe it are well-grounded in recently declassified government reports.[3]

More importantly, I lived it. And I never want to live through that particular Groundhog Day again. That's why I'm here.

I am afraid that hyped and distorted press reports orchestrated by Edward Snowden and his allies may cause us—or other nations—to construct new restraints on our intelligence gathering, restraints that will leave us vulnerable to another security disaster.

I. Intelligence Gathering Under Law

The problem we are discussing today has roots in a uniquely American and fairly recent experiment—writing detailed legal rules to govern the conduct of foreign intelligence. This is new, even for a country that puts great faith in law.

The Americans who fought World War II had a different view; they thought that intelligence couldn't be conducted under any but the most general legal constraints. This may have been a reaction to a failure of law in the run-up to World War II, when U.S. codebreakers were forbidden to intercept Japan's coded radio communications because Section 605 of the Federal Communications Act made such intercepts illegal. Finally, in 1939, Gen. George C. Marshall told Navy intelligence officers to ignore the law.[4] The military successes that followed made the officers look like heroes, not felons.

That view held for nearly forty years, but it broke down in the wake of Watergate, when Congress took a close look at the intelligence community, found abuses, and in 1978 adopted the first detailed legal regulation of intelligence gathering in history—the Foreign Intelligence Surveillance Act. No other nation has ever tried to regulate intelligence so publicly and so precisely in law.

Forty years later, though, we're still finding problems with this experiment. One of them is that law changes slowly while

---

Stewart A. Baker is a partner in the Washington office of Steptoe & Johnson LLP. He was previously the Department of Homeland Security's first Assistant Secretary for Policy. His memoir of his time at DHS is entitled Skating on Stilts: Why We Aren't Stopping Tomorrow's Terrorism.

The article has been adapted from testimony before the U.S. Senate Judiciary Committee on July 31, 2013. His complete testimony is available at http://www.judiciary.senate.gov/pdf/7-31-13BakerTestimony.pdf.

technology changes quickly. That usually means Congress has to change the law frequently to keep up. But in the context of intelligence, it's often hard to explain *why* the law needs to be changed, let alone to write meaningful limits on collection without telling our intelligence targets a lot about our collection techniques. A freewheeling and prolonged debate—and does Congress have any other kind?—will give them enough time and knowledge to move their communications away from technologies we've mastered and into technologies that thwart us. The result won't be intelligence under law; it will be law without intelligence.

Much of what we've read in the newspapers lately about the NSA and FISA is the product of this tension. Our intelligence capabilities—and our intelligence gaps—are mostly new since 1978, forcing the government, including Congress, to find ways to update the law without revealing how we gather intelligence.

* * *

II. What Next?

Setting aside the half-truths and the hype, what does the current surveillance flap tell us about the fundamental question we've faced since 1978—how to gather intelligence under law?

Regulating Technology—What Works and What Doesn't

First, since American intelligence has always been at its best in using new technologies, intelligence law will always be falling out of date, and the more specific its requirements the sooner it will be outmoded.

Second, we aren't good at regulating government uses of technology. That's especially a risk in the context of intelligence, where the government often pushes the technological envelope. The privacy advocates who tend to dominate the early debates about government and technology suffer from a sort of ideological technophobia, at least as far as government is concerned. Even groups that claim to embrace the future want government to cling to the past. And the laws they help pass reflect that failing.

To take an old example, in the 1970s, well before the personal computer and the Internet, privacy campaigners persuaded the country that the FBI's newspaper clipping files about U.S. citizens were a threat to privacy. Sure, the information was public, they acknowledged, but gathering it all in one file was viewed as sinister. And maybe it was; it certainly gave J. Edgar Hoover access to embarrassing information that had been long forgotten everywhere else. So in the wake of Watergate, the attorney general banned the practice in the absence of some investigative predicate.

The ban wasn't reconsidered for twenty-five years. And so, in 2001, when search engines had made it possible for anyone to assemble a clips file about anyone in seconds, the one institution in the country that could not print out the results of its Internet searches about Americans was the FBI. This was bad for our security, and it didn't protect anyone's privacy either.

Now we're hearing calls to regulate how the government uses big data in security and law enforcement investigations. This is about as likely to protect our privacy as reinstating the ban on clips files. We can pass laws turning the federal government into an Amish village, but big data is here to stay, and it will be used by everyone else. Every year, data gets cheaper to collect and cheaper to analyze. You can be sure that corporate America is taking advantage of this remorseless trend. The same is true of the cyberspies in China's Peoples' Liberation Army.

If we're going to protect privacy, we won't succeed by standing in front of big data shouting "Stop!" Instead, we need to find privacy tools—even big data privacy tools—that take advantage of technological advances. The best way to do that, in my view, was sketched a decade ago by the Markle Foundation Task Force on National Security, which called on the government to use new technologies to better monitor government employees who have access to sensitive information.[5] We need systems that audit for data misuse, that flag questionable searches, and that require employees to explain why they are seeking unusual data access. That's far more likely to provide effective protection against misuse of private data than trying to keep cheap data out of government hands. The federal government has in fact made progress in this area; that's one reason that the minimization and targeting rules could be as detailed as they are. But it clearly needs to do better. A proper system for auditing access to restricted data would not just improve privacy enforcement, it likely would have flagged both Bradley Manning and Edward Snowden for their unusual network browsing habits.

* * *

Thirty-five years of trying to write detailed laws for intelligence gathering have revealed just how hard that exercise is—and why so few nations have tried to do it. In closing, let me offer some quick thoughts on two proposals that would "fix" FISA by doubling down on this approach.

One idea is to declassify FISA Court opinions. Another is to appoint outside lawyers with security clearances who can argue against the government. The problem with these proposals is that they're not likely to persuade the FISA doubters that the law protects their rights. But they are likely to put sources and methods at greater risk.

Declassification of the FISA Court opinions already happens, but only when the opinion can be edited so that the public version does not compromise sources and methods. The problem is that most opinions make law only by applying legal principles to particular facts. In the FISA context, those facts are almost always highly classified, so it's hard to explain the decision without getting very close to disclosing sources and methods. To see what I mean, I suggest this simple experiment. Let's ask the proponents of declassification to write an unclassified opinion approving the current Section 215 program—without giving away details about how the program works. I suspect that the result will be at best cryptic; it will do little to inspire public trust but much to spur speculation and risk to sources and methods.

What about appointing counsel in FISA matters? Well, we don't appoint counsel to protect the rights of Mafia chieftains or drug dealers. Wiretap orders and search warrants aimed at them are reviewed by judges without any advocacy on behalf of

the suspect. Why in the world would we offer more protection to al Qaeda?

I understand the argument that appointing counsel will provide a check on the government, whose orders may never see the light of day or be challenged in a criminal prosecution. But the process is already full of such checks. The judges of the FISA Court have cleared law clerks who surely see themselves as counterweights to the government's lawyers. The government's lawyers themselves come not from the intelligence community but from a Justice Department office that sees itself as a check on the intelligence community and feels obligated to give the FISA Court facts and arguments that it would not offer in an adversary hearing. There may be a dozen offices that think their job is to act as a check on the intelligence community's use of FISA: inspectors general, technical compliance officers, general counsel, intelligence community staffers, and more. To that army of second-guessers, are we really going to add yet another lawyer, this time appointed from outside the government?

For starters, we won't be appointing a lawyer. There certainly are outside lawyers with clearances. I'm one. But senior partners don't work alone, and there are very few nongovernment citecheckers and associates and typists with clearances. Either we'll have to let intercept orders sit for months while we try to clear a law firm's worth of staff—along with their computer systems, Blackberries, and filing systems—or we'll end up creating an office to support the advocates.

And who will fill that office? I've been appointed to argue cases, even one in the Supreme Court, and I can attest that deciding what arguments to make has real policy implications. Do you swing for the fences and risk a strikeout, or do you go for a bunt single that counts as a win but might change the law only a little? These are decisions on which most lawyers must consult their clients, or, if they work for governments, their political superiors. But the lawyers we appoint in the FISA Court will have no superiors and effectively no clients.

To update the old saw, a lawyer who represents himself has an ideologue for a client. In questioning the wisdom of special prosecutors, Justice Scalia noted the risk of turning over prosecutorial authority to high-powered private lawyers willing to take a large pay cut and set aside their other work for an indeterminate time just to be able to investigate a particular president or other official. Well, who would want to turn over the secrets of our most sensitive surveillance programs, and the ability to suggest policy for those programs, to high-powered lawyers willing to take a large pay cut and set aside their other work for an indeterminate period just to be able to argue that the programs are unreasonable, overreaching, and unconstitutional?

Neither of these ideas will, in my view, add a jot to public trust in the intelligence gathering process. But they will certainly add much to the risk that intelligence sources and methods will be compromised. For that reason, we should approach them with the greatest caution.

Endnotes

1 Timothy Lynch, *Dereliction Of Duty: The Constitutional Record of President Clinton*, Cato Policy Analysis No. 271 (March 31, 1997), http://www.cato.org/pubs/pas/pa-271.html.

2 Hon. Royce C. Lamberth, Presiding Judge of the Foreign Intelligence Surveillance Court, Address Before the American Bar Ass'n Standing Comm. on Law and Nat'l Sec. (April 4, 1997), in 19 American Bar Ass'n Nat'l Sec. L. Rep. 2, May 1997, at 1-2.

3 Stewart Baker, Skating on Stilts 66-69 (2010).

4 David Kahn, The Codebreakers: The Comprehensive History of Secret Communication from Ancient Times to the Internet 12 (2d ed. 1996).

5 The Task Force's first report called for the federal government to adopt

> robust permissioning structures and audit trails that will help enforce appropriate guidelines. These critical elements could employ a wide variety of authentication, certification, verification, and encryption technologies. Role-based permissions can be implemented and verified through the use of certificates, for example, while encryption can be used to protect communications and data transfers. … Auditing tools that track how, when, and by whom information is accessed or
>
> used ensure accountability for network users. These two safeguards—permissioning and auditing—will free participants to take initiatives within the parameters of our country's legal, cultural, and societal norms.

Markle Foundation Task Force, Protecting America's Freedom in the Information Age 17 (October 2002), http://www.markle.org/sites/default/files/nstf_full.pdf.

Workshop Regarding Surveillance Programs Operated Pursuant to Section 215 of the USA PATRIOT Act and Section 702 of the Foreign Intelligence Surveillance Act

Privacy and Civil Liberties Oversight Board

July 9, 2013

*Nathan A. Sales**

Chairman Medine and members of the Board, thank you for inviting me to participate in this workshop. The NSA's recently disclosed surveillance programs raise a number of vitally important questions about the interplay between the government's compelling need to prevent terrorist attacks and our nation's fundamental commitment to civil liberties and privacy. Briefly summarized, my statement will address the potential national security benefits of bulk data collection; it will propose some guiding principles to help ensure that any such surveillance regime is consistent with basic privacy and civil liberties values; and it will offer some preliminary thoughts on how to modify the NSA programs to ensure that they better comport with these first principles. I understand that the Board is especially interested in policy recommendations, so my statement will focus more on policy considerations than legal analysis.

While programmatic surveillance can be an important counterterrorism tool, it also—given the sweeping scope of the data collection on which it usually relies—has the potential to raise profound concerns about civil liberties and privacy. It therefore becomes critical to establish a set of first principles to govern when and how this monitoring is to be conducted. It is especially important to think about these baseline rules now, when programmatic surveillance is still in its relative youth. This will allow the technique to be nudged in privacy-protective directions as it develops into maturity. The critical question is how to take advantage of the potentially significant national security benefits offered by programmatic surveillance without running afoul of fundamental civil liberties and privacy values. In other words, what can be done to domesticate programmatic surveillance?

This is not the place to flesh out the precise details of the ideal surveillance regime, but we can identify certain basic principles that policymakers and others should consider when thinking about bulk data collection and analysis. Two broad categories of principles should govern any such system; one concerns its formation, the other its operation. First, there are the *architectural* or *structural* considerations—the principles that address when programmatic surveillance should take place, the process by which such a regime should be adopted, and how the system should be organized. Second, there are the *operational* considerations—the principles that inform the manner in which programmatic surveillance should be carried out in practice.

A.

As for the structural considerations, one of the most important is what might be called an *anti-unilateralism* principle. A system of programmatic surveillance should not be put into effect simply on the say-so of the executive branch, but rather should be a collaborative effort that involves Congress (in the form of authorizing legislation) and the judiciary (in the form of a FISA court order reviewing and approving the executive's proposed surveillance activities). An example of the former is FISA itself, which Congress enacted with the executive's (perhaps reluctant) consent in 1978. FISA's famously convoluted definition of "electronic surveillance"[1] can be seen as a congressional effort to preserve the NSA's preexisting practice of collecting certain foreign-foreign and foreign-domestic communications without prior judicial approval. An example of the latter concerns the Terrorist Surveillance Program. After that program came under harsh criticism when its existence was revealed in late 2005, the executive branch persuaded the FISA court to issue orders allowing the program to proceed subject to various clarifications and limits.[2] That accommodation eventually proved unworkable, and the executive then worked with Congress to put the program on a more solid legislative footing through the temporary Protect America Act of 2007 and the permanent FISA Amendments Act of 2008.

Anti-unilateralism is important for several reasons. For one, the risk of executive overreach is lessened if that branch must enlist its partners before commencing a new surveillance initiative. Congress might decline to permit bulk collection in circumstances where it concludes that ordinary, individualized monitoring would suffice, or it might authorize programmatic surveillance subject to various privacy protections. In addition, inviting many voices to the decisionmaking table increases the probability of sound policy outcomes. More participants can also help mitigate groupthink tendencies. In short, if we're going to engage in programmatic surveillance, it should be the result of give and take among all three branches of the federal government (or at least between its two political branches), not the result of executive edict.

A second structural principle follows from the first: Programmatic surveillance should, where possible, have *explicit statutory authorization*. Congress does not "hide elephants in mouseholes,"[3] the saying goes, and we should not presume that Congress meant to conceal its approval of a useful but potentially controversial programmatic surveillance system in the penumbrae and interstices of obscure federal statutes. Instead, Congress normally should use express and specific legislation when it wishes the executive branch to engage in bulk data

Nathan A. Sales is an Assistant Professor of Law at George Mason University. He was previously the first Deputy Assistant Secretary for Policy Development at the U.S Department of Homeland Security, and from 2001-2003 he served at the Office of Legal Policy at the U.S Department of Justice, where he focused on counterterrorism policy and helped draft the USA PATRIOT Act.

The article has been adapted from testimony at the Privacy and Civil Liberties Oversight Board workshop on July 9, 2013.

collection. Clear laws will help remove any doubt about the authorized scope of the approved surveillance. Express congressional backing also helps bring an air of legitimacy to the monitoring. And a requirement that programmatic surveillance usually should be approved by clear legislation helps promote accountability by minimizing the risk of congressional shirking.

Of course, exacting legislative clarity may not be possible in all cases; sometimes, explicit statutory language might reveal operational details and compromise intelligence sources and methods or provoke a diplomatic row. But clarity often will be feasible, and the Protect America Act and FISA Amendments Act are good examples of what the process could look like. In both cases, Congress clearly and unambiguously approved monitoring that the executive branch previously claimed[4] was implicitly authorized by a combination of FISA (which at the time made it unlawful to engage in electronic surveillance "except as authorized by statute"[5]), the September 18, 2001 Authorization for Use of Military Force (which authorizes the president to use "all necessary and appropriate force" against those responsible for 9/11[6]), and the Supreme Court's decision in *Hamdi v. Rumsfeld* (which interpreted the AUMF's reference to "all necessary and appropriate force" to include "fundamental and accepted" incidents of war, such as detention[7]).

Next, there is the question of *transparency*. Whenever possible, programmatic surveillance systems should be adopted through open and transparent debates that allow an informed public to meaningfully participate. The systems also should be operated in as transparent a manner as possible. This in turn requires the government to reveal enough information about the proposed surveillance, even if at a fairly high level of generality, that the public is able to effectively weigh its benefits and costs. Transparency is important because it helps promote accountability; it enables the public to hold their representatives in Congress and in the executive branch responsible for the choices they make. Transparency also fosters democratic participation, ensuring that the people are ultimately able to decide what our national security policies should be. And it can help dispel suspicions about programs that otherwise might seem nefarious. Again, perfect transparency will not always be feasible—a public debate about the fine-grained details of proposed surveillance can compromise extremely sensitive intelligence sources and methods. But transparency should be the default rule, and even where the government's operational needs rule out detailed disclosures, a generic description of the proposed program is better than none at all.

Finally, any programmatic surveillance regime should observe an *anti-mission-creep* principle. Bulk data collection should only be used to investigate and prevent terrorism, espionage, and other serious threats to the national security. It should be off limits in regular criminal investigations. And if programmatic surveillance happens to turn up evidence of low-grade criminal activity, intelligence authorities normally should not be able to refer it to their law enforcement counterparts—though there should be an exception for truly grave crimes, such as offenses involving a risk of death or serious bodily injury and crimes involving the exploitation of children. This is a simple matter of costs and benefits. The upside of preventing deadly terrorist attacks and other national security perils can be so significant that we as a nation may be willing to resort to extraordinary investigative techniques like bulk data collection. But the calculus looks very different where the promised upside is prosecuting ordinary crimes like income tax evasion or insurance fraud. We might be willing to tolerate an additional burden on our privacy interests to stop the next 9/11, but not to stop tax cheats and fraudsters.

B.

As for the operational considerations, among the most important is the need for *external checks* on programmatic surveillance, whether judicial, legislative, or both. In particular, bulk data collection should have to undergo some form of judicial review, such as by the FISA court, in which the government demonstrates that it meets the Fourth Amendment standards that apply to the acquisition of the data in question. Ideally, the judiciary would give its approval before collection begins. But this will not always be possible, in which case timely post-collection judicial review will have to suffice. (FISA contains a comparable mechanism for temporary warrantless surveillance in emergency situations.) Programmatic surveillance also should be subject to robust congressional oversight. This could take a variety of forms, including informal consultations with congressional leadership and the appropriate committees when designing the surveillance regime, as well as regular briefings to appropriate personnel on the operation of the system and periodic oversight hearings.

Oversight by the courts and Congress provides an obvious, first-order level of protection for privacy and civil liberties—an external veto serves as a direct check on possible executive misconduct, such as engaging in monitoring when it is not justified or using surveillance against political enemies or dissident groups. Judicial and legislative checks also offer a less noticed but equally important second-order form of protection. The mere possibility of an outsider's veto can have a chilling effect on executive misconduct, discouraging officials from questionable activities that would have to undergo, and might not survive, external review. Moreover, external checks can channel the executive's scarce resources into truly important surveillance and away from relatively unimportant monitoring. This is so because oversight increases the executive's costs of collecting bulk data—e.g., preparing a surveillance application, persuading the judiciary to approve it, briefing the courts and Congress about how the program has been implemented, and so on. These increased costs encourage the executive to prioritize collection that is expected to yield truly valuable intelligence and, conversely, to forego collection that is expected to produce information of lesser value.

Of course, judicial review in the context of bulk collection won't necessarily look the same as it does in the familiar setting of individualized monitoring of specific targets. If investigators want to examine a particular terrorism suspect's telephony metadata, they apply to the FISA court for a pen register/trap and trace order upon a showing that the information sought is relevant to an ongoing national security investigation. But, as explained above, that kind of particularized showing usually

won't be possible where authorities are dealing with unknown threats, and where the very purpose of the surveillance is to identify the threats. In these situations, reviewing courts may find it necessary to allow the government to collect large amounts of data without an individualized showing of relevance. This doesn't mean that privacy safeguards must be abandoned and the executive given free rein. Instead of serving as a gatekeeper for the government's collection of data, courts could require that authorities demonstrate some level of individualized suspicion before they access the data that has been collected. Protections for privacy and civil liberties can migrate from the front end of the intelligence cycle to the back end.

In more general terms, because programmatic surveillance involves the collection of large troves of data, it inevitably means some dilution of the familiar ex ante restrictions that protect privacy by constraining the government from acquiring information in the first place. It therefore becomes critically important to devise meaningful ex post safeguards that can achieve similar forms of privacy protection. In short, meaningful restrictions on the government's ability to use data that it has gathered must substitute for restrictions on the government's ability to gather that data at all; what I have elsewhere called *use limits* must stand in for *collection limits*.[8]

In addition to oversight by outsiders, a programmatic surveillance regime also should feature a system of *internal checks* within the executive branch, to review collection before it occurs, after the fact, or both. These sorts of internal restraints are familiar features of the post-1970s national security state, and there is no reason to exempt programmatic surveillance. As for the ex ante checks, internal watchdogs should be charged with scrutinizing proposed bulk collection to verify it complies with the applicable constitutional and statutory rules, and also to ensure that appropriate protections are in place for privacy and civil liberties. The Justice Department's Office of Intelligence is a well known example. The office, which presents the government's surveillance applications to the FISA court, subjects proposals to exacting scrutiny, sometimes including multiple rounds of revisions, with the goal of increasing the likelihood of surviving judicial review. Indeed, the office has a strong incentive to ensure that the applications it presents are in good order, so as to preserve its credibility with the FISA court.

Ex post checks include such common mechanisms as agency-level inspectors general, who can be charged with auditing bulk collection programs and also making policy recommendations to improve their operation, as well as entities like the Privacy and Civil Liberties Oversight Board, which perform similar functions across the executive branch as a whole. Another important ex post check is to offer meaningful whistleblower protections to officials who know about programs that violate constitutional or statutory rules. Allowing officials to bring their concerns to ombudsmen within the executive branch can help root out lawlessness and also relieve the felt necessity of leaking information about highly classified programs to the media.

These and other mechanisms can be an effective way of preventing executive misconduct. Done properly, internal checks can achieve all three of the benefits promised by traditional judicial and legislative oversight—executive branch watchdogs can veto surveillance they conclude would be unlawful, the mere possibility of such vetoes can chill overreach, and increasing the costs of monitoring can redirect scarce resources toward truly important surveillance. External and internal checks thus operate together as a system; the two types of restraints are rough substitutes for one another. If outside players like Congress and the courts are subjecting the executive's programmatic surveillance activities to especially rigorous scrutiny, the need for comparably robust safeguards within the executive branch tends to diminish. Conversely, if the executive's discretion is constrained internally through strict approval processes, audit requirements, and so on, the legislature and judiciary may choose not to hold the executive to the exacting standards they otherwise would. In short, certain situations may see less need to use traditional interbranch separation of powers and checks and balances to protect privacy and civil liberties, because the executive branch itself is subject to an "internal separation of powers."[9]

A word of caution. It's important not to take these in-house review mechanisms too far. Internal oversight can do more than deter executive branch overreach. It can also deter necessary national security operations, with potentially deadly results. The pre-9/11 information sharing wall is a notorious example of an internal check gone awry—executive branch lawyers interpreted FISA to sharply restrict intelligence officials from coordinating or sharing information with their law enforcement counterparts, leading one prophetic FBI agent to lament on the eve of 9/11 that "someday somebody will die."[10] There are other examples as well. In the 1990s, executive branch lawyers vetoed CIA plans to use targeted killing against Osama bin Laden, and JAG lawyers have occasionally ruled out air strikes on policy grounds even though they would be permissible under the laws of war.[11] There is no universally applicable answer to the question, *how much internal oversight is enough?* Too little imperils privacy, too much threatens security. The right balance cannot be known a priori, but rather must be struck on a case by case basis taking account of the highly contingent and unique circumstances presented by a given surveillance program, the threat it seeks to combat, and other factors.

A third operational consideration is the need for strong *minimization requirements*. Virtually all surveillance raises the risk that officials will intercept innocuous data in the course of gathering evidence of illicit activity. Inevitably, some chaff will be swept up with the wheat. The risk is especially acute with programmatic surveillance, in which the government assembles large amounts of data in the search for clues about a small handful of terrorists, spies, and other threats to the national security. Minimization is one way to deal with the problem. Minimization rules limit what the government may do with data that does not appear pertinent to a national security investigation—e.g., how long it may be retained, the conditions under which it will be stored, the rules for accessing it, the purposes for which it may be used, the entities with which it may be shared, and so on. Congress appropriately has required intelligence officials to adopt minimization procedures, both under FISA's longstanding particularized surveillance regime and under the more recent

authorities permitting bulk collection. But the rules need not be identical. Because programmatic surveillance often involves the acquisition of a much larger trove of non-pertinent information, the minimization rules for bulk collection ideally would contain stricter limits on the use of information unrelated to national security threats. In other words, the minimization procedures should reflect the *anti-mission-creep* principle described above.

Finally, programmatic surveillance systems should have *technological safeguards* that protect privacy and civil liberties by restricting access to sensitive information and tracking what officials do with it. Permissioning and authentication technologies can help ensure that sensitive databases are only available to officials who need them to perform various counterterrorism functions. And auditing tools can track who accesses the information, when, in what manner, and for what purposes. These kinds of mechanisms show promise but have a mixed record at preventing unauthorized access and use of sensitive data. The use of access logs helped the State Department quickly identify and discipline the outside contractors who in 2008 improperly accessed the private passport files of various presidential candidates. But people like Edward Snowden and Bradley Manning obviously have been able to exfiltrate huge amounts of classified information from protected systems, either because access controls were not in place or because they were able to evade them. Even if technological controls are not now an infallible safeguard against abuse, the basic principle seems sound: A commitment to privacy can be baked into a programmatic surveillance regime at the level of systems architecture.

* * *

Bulk data collection is probably here to stay. Programmatic surveillance that aims at identifying previously unknown terrorists and spies has the potential to be an important addition to the national security toolkit. And in an era where private companies like Amazon and Google assemble detailed digital dossiers to predict their customers' buying habits, it's more or less inevitable that counterterrorism officials will want to take advantage of the same sorts of technologies to stop the next 9/11. That's why it's critical to establish a baseline set of rules to govern the creation and operation of any system of programmatic surveillance. These first principles can ensure that the government is equipped a valuable tool for preventing terrorist atrocities while simultaneously preserving our national commitment to civil liberties and privacy.

Endnotes

1 50 U.S.C. § 1801(f).

2 David Kris, *A Guide to the New FISA Bill, Part II*, Balkinization (July 29, 2013, 12:45 PM), http://balkin.blogspot.com/2008/06/guide-to-new-fisa-bill-part-ii.html.

3 Whitman v. Am. Trucking Ass'ns, 531 U.S. 457, 468 (2001).

4 Letter from William E. Moschella, Assistant Att'y Gen., Off. of Legis. Aff., U.S. Dep't of Justice., to Pat Roberts, Chairman, Senate Select Comm. on Intelligence, et al. (Dec. 22, 2005), *available at* http://www.fas.org/irp/agency/doj/fisa/doj122205.pdf.

5 50 U.S.C. § 1809(a)(1).

6 Pub. L. No. 107-40, § 2(a), 115 Stat. 224 (2001).

7 542 U.S. 507, 518 (2004).

8 Nathan Alexander Sales, *Run for the Border: Laptop Searches and the Fourth Amendment*, 43 U. Rich. L. Rev. 1091, 1124-27 (2009).

9 Neal Kumar Katyal, *Internal Separation of Powers: Checking Today's Most Dangerous Branch from Within*, 115 Yale L.J. 2314 (2006).

10 National Commission on Terrorist Attacks Upon the United States, The 9/11 Commission Report 271 (2004).

11 Nathan Alexander Sales, *Self Restraint and National Security*, 6 J. Nat'l Sec. L. & Pol'y 227, 247-56 (2012).

Before
The House Committee on the Judiciary

Oversight Hearing on
The Administration's Use of FISA Authorities

July 17, 2013

Jameel Jaffer & Laura W. Murphy***

On behalf of the American Civil Liberties Union (ACLU), its hundreds of thousands of members, and its fifty-three affiliates nationwide, thank you for inviting the ACLU to testify before the Committee.

Over the last six weeks it has become clear that the National Security Agency (NSA) is engaged in far-reaching, intrusive, and unlawful surveillance of Americans' telephone calls and electronic communications. That the NSA is engaged in this surveillance is the result of many factors. The Foreign Intelligence Surveillance Act (FISA) affords the government sweeping power to monitor the communications of innocent people. Excessive secrecy has made congressional oversight difficult and public oversight impossible. Intelligence officials have repeatedly misled the public, Congress, and the courts about the nature and scope of the government's surveillance activities. Structural features of the Foreign Intelligence Surveillance Court (FISC) have prevented that court from serving as an effective guardian of individual rights. And the ordinary federal courts have improperly used procedural doctrines to place the NSA's activities beyond the reach of the Constitution.

To say that the NSA's activities present a grave danger to American democracy is no overstatement. Thirty-seven years ago, after conducting a comprehensive investigation into the intelligence abuses of the previous decades, the Church Committee warned that inadequate regulations on government surveillance "threaten[ed] to undermine our democratic society and fundamentally alter its nature." This warning should have even more resonance today, because in recent decades the NSA's resources have grown, statutory and constitutional limitations have been steadily eroded, and the technology of surveillance has become exponentially more powerful.

Because the problem Congress confronts today has many roots, there is no single solution to it. It is crucial, however, that Congress take certain steps immediately. It should amend relevant provisions of FISA to prohibit suspicionless, "dragnet" monitoring or tracking of Americans' communications. It should require the publication of past and future FISC opinions insofar as they evaluate the meaning, scope, or constitutionality of the foreign-intelligence laws. It should ensure that the public has access to basic information, including statistical information, about the government's use of new surveillance authorities. It should also hold additional hearings to consider further amendments to FISA—including amendments to make FISC proceedings more transparent.

** Deputy Legal Director of the American Civil Liberties Union Foundation*

*** Director, Washington Legislative Office, American Civil Liberties Union*

I. Metadata Surveillance under Section 215 of the Patriot Act

On June 5, 2013, *The Guardian* disclosed a previously secret FISC order that compels a Verizon subsidiary, Verizon Business Network Services (VBNS), to supply the government with records relating to every phone call placed on its network between April 25, 2013 and July 19, 2013.[1] The order directs VBNS to produce to the NSA "on an ongoing daily basis . . . all call detail records or 'telephony metadata'" relating its customers' calls, including those "wholly within the United States."[2] As many have noted, the order is breathtaking in its scope. It is as if the government had seized every American's address book—with annotations detailing which contacts she spoke to, when she spoke with them, for how long, and (possibly) from which locations.

News reports since the disclosure of the VBNS order indicate that the mass acquisition of Americans' call details extends beyond customers of VBNS, encompassing subscribers of the country's three largest phone companies: Verizon, AT&T, and Sprint.[3] Members of the congressional intelligence committees have confirmed that the order issued to VBNS is part of a broader program under which the government has been collecting the telephone records of essentially all Americans for at least seven years.[4]

A. The metadata program is not authorized by statute

The metadata program has been implemented under Section 215 of the Patriot Act—sometimes referred to as FISA's "business records" provision—but this provision does not permit the government to track all Americans' phone calls, let alone over a period of seven years.

As originally enacted in 1998, FISA's business records provision permitted the FBI to compel the production of certain business records in foreign intelligence or international terrorism investigations by making an application to the FISC. *See* 50 U.S.C. §§ 1861-62 (2000 ed.). Only four types of records could be sought under the statute: records from common carriers, public accommodation facilities, storage facilities, and vehicle rental facilities. 50 U.S.C. § 1862 (2000 ed.). Moreover, the FISC could issue an order only if the application contained "specific and articulable facts giving reason to believe that the person to whom the records pertain[ed] [was] a foreign power or an agent of a foreign power." *Id*.

The business records power was considerably expanded by the Patriot Act.[5] Section 215 of that Act, now codified in 50 U.S.C. § 1861, permitted the FBI to make an application to the FISC for an order requiring

> the production of *any tangible things* (including books, records, papers, documents, and other items)

> for an investigation to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities . . . .

50 U.S.C. § 1861(a)(1) (emphasis added).

No longer limited to four discrete categories of business records, the new law authorized the FBI to seek the production of "any tangible things." *Id*. It also authorized the FBI to obtain orders without demonstrating reason to believe that the target was a foreign power or agent of a foreign power. Instead, it permitted the government to obtain orders where tangible things were "sought for" an authorized investigation. P.L. 107-56, § 215. This language was further amended by the USA PATRIOT Improvement and Reauthorization Act of 2005, P.L. 109-177, § 106(b). Under the current version of the business records provision, the FBI must provide "a statement of facts showing that there are reasonable grounds to believe that the tangible things sought are *relevant*" to a foreign intelligence, international terrorism, or espionage investigation. 50 U.S.C. § 1861(b)(2)(A) (emphasis added).[6]

While the Patriot Act considerably expanded the government's surveillance authority, Section 215 does not authorize the metadata program. First, whatever "relevance" might allow, it does not permit the government to cast a seven-year dragnet over the records of every phone call made or received by any American. Indeed, to say that Section 215 authorizes this surveillance is to deprive the word "relevance" of any meaning. The government's theory appears to be that some of the information swept up in the dragnet might become relevant to "an authorized investigation" at some point in the future. The statute, however, does not permit the government to collect information on this basis. *Cf.* Jim Sensenbrenner, *This Abuse of the Patriot Act Must End*, Guardian, June 9, 2013, http://bit.ly/18iDA3x ("[B]ased on the scope of the released order, both the administration and the FISA court are relying on an unbounded interpretation of the act that Congress never intended."). The statute requires the government to show a connection between the records it seeks and some specific, existing investigation.

Indeed, the changes that Congress made to the statute in 2006 were meant to ensure that the government did not exploit ambiguity in the statute's language to justify the collection of sensitive information not actually connected to some authorized investigation. As Senator Jon Kyl put it in 2006, "We all know the term 'relevance.' It is a term that every court uses. The relevance standard is exactly the standard employed for the issuance of discovery orders in civil litigation, grand jury subpoenas in a criminal investigation."[7]

As Congress recognized in 2006, relevance is a familiar standard in our legal system. It has never been afforded the limitless scope that the executive branch is affording it now. Indeed, in the past, courts have carefully policed the outer perimeter of "relevance" to ensure that demands for information are not unbounded fishing expeditions. *See, e.g.*, *In re Horowitz*, 482 F.2d 72, 79 (2d Cir. 1973) ("What is more troubling is the matter of relevance. The [grand jury] subpoena requires production of all documents contained in the files, without any attempt to define classes of potentially relevant documents or any limitations as to subject matter or time period.").[8] The information collected by the government under the metadata program goes far beyond anything a court has ever allowed under the rubric of "relevance."[9]

B. The metadata program is unconstitutional

President Obama and intelligence officials have been at pains to emphasize that the government is collecting metadata, not content. The suggestion that metadata is somehow beyond the reach of the Constitution, however, is not correct. For Fourth Amendment purposes, the crucial question is not whether the government is collecting content or metadata but whether it is invading reasonable expectations of privacy. In the case of bulk collection of Americans' phone records, it clearly is.

The Supreme Court's recent decision in *United States v. Jones*, 132 S. Ct. 945 (2012), is instructive. In that case, a unanimous Court held that long-term surveillance of an individual's location constituted a search under the Fourth Amendment. The Justices reached this conclusion for different reasons, but at least five Justices were of the view that the surveillance infringed on a reasonable expectation of privacy. Justice Sotomayor observed that tracking an individual's movements over an extended period allows the government to generate a "precise, comprehensive record" that reflects "a wealth of detail about her familial, political, professional, religious, and sexual associations." *Id*. (Sotomayor, J., concurring).

The same can be said of the tracking now taking place under Section 215. Call records can reveal personal relationships, medical issues, and political and religious affiliations. Internet metadata may be even more revealing, allowing the government to learn which websites a person visits, precisely which articles she reads, whom she corresponds with, and whom *those* people correspond with.

The long-term surveillance of metadata constitutes a search for the same reasons that the long-term surveillance of location was found to constitute a search in *Jones*. In fact, the surveillance held unconstitutional in *Jones* was narrower and shallower than the surveillance now taking place under Section 215. The location tracking in *Jones* was meant to further a specific criminal investigation into a specific crime, and the government collected information about one person's location over a period of less than a month. What the government has implemented under Section 215 is an indiscriminate program that has already swept up the communications of millions of people over a period of seven years.

Some have defended the metadata program by reference to the Supreme Court's decision in *Smith v. Maryland*, 442 U.S. 735 (1979), which upheld the installation of a pen register in a criminal investigation. The pen register in *Smith,* however, was very primitive—it tracked the numbers being dialed, but it didn't indicate which calls were completed, let alone the duration of the calls. Moreover, the surveillance was directed at a single criminal suspect over a period of less than two days. The police were not casting a net over the whole country.

Another argument that has been offered in defense of the

metadata program is that, though the NSA collects an immense amount of information, it examines only a tiny fraction of it. But the Fourth Amendment is triggered by the *collection* of information, not simply by the querying of it. The NSA cannot insulate this program from Fourth Amendment scrutiny simply by promising that Americans' private information will be safe in its hands. The Fourth Amendment exists to prevent the government from acquiring Americans' private papers and communications in the first place.

Because the metadata program vacuums up sensitive information about associational and expressive activity, it is also unconstitutional under the First Amendment. The Supreme Court has recognized that the government's surveillance and investigatory activities have an acute potential to stifle association and expression protected by the First Amendment. *See, e.g.*, *United States v. U.S. District Court*, 407 U.S. 297 (1972). As a result of this danger, courts have subjected investigatory practices to "exacting scrutiny" where they substantially burden First Amendment rights. *See, e.g.*, *Clark v. Library of Congress,* 750 F.2d 89, 94 (D.C. Cir. 1984) (FBI field investigation); *In re Grand Jury Proceedings*, 776 F.2d 1099, 1102-03 (2d Cir. 1985) (grand jury subpoena). The metadata program cannot survive this scrutiny. This is particularly so because all available evidence suggests that the program is far broader than necessary to achieve the government's legitimate goals. *See, e.g.*, Press Release, *Wyden, Udall Question the Value and Efficacy of Phone Records Collection in Stopping Attacks*, June 7, 2013, http://1.usa.gov/19Q1Ng1 ("As far as we can see, all of the useful information that it has provided appears to have also been available through other collection methods that do not violate the privacy of law-abiding Americans in the way that the Patriot Act collection does.").

C. Congress should amend Section 215 to prohibit suspicionless, dragnet collection of "tangible things"

As explained above, the metadata program is neither authorized by statute nor constitutional. As the government and FISC have apparently found to the contrary, however, the best way for Congress to protect Americans' privacy is to narrow the statute's scope. The ACLU urges Congress to amend Section 215 to provide that the government may compel the production of records under the provision only where there is a close connection between the records sought and a foreign power or agent of a foreign power. Several bipartisan bills now in the House and Senate should be considered by this Committee and Congress at large. The LIBERT-E Act, H.R. 2399, 113th Cong. (2013), sponsored by Ranking Member Conyers, Rep. Justin Amash, and forty others, would tighten the relevance requirement, mandating that the government supply "specific and articulable facts showing that there are reasonable grounds to believe that the tangible things sought are relevant and material," and that the records sought "pertain only to an individual that is the subject of such investigation." A bill sponsored by Senators Udall and Wyden would similarly tighten the required connection between the government's demand for records and a foreign power or agent of a foreign power. Congress could also consider simply restoring some of the language that was deleted by the Patriot Act—in particular, the language that required the government to show "specific and articulable facts giving reason to believe that the person to whom the records pertain[ed] [was] a foreign power or an agent of a foreign power."

II. Electronic Surveillance under Section 702 of FISA

The metadata program is only one part of the NSA's domestic surveillance activities. Recent disclosures show that the NSA is also engaged in large-scale monitoring of Americans' electronic communications under Section 702 of FISA, which codifies the FISA Amendments Act of 2008.[10] Under this program, labeled "PRISM" in NSA documents, the government collects emails, audio and video chats, photographs, and other internet traffic from nine major service providers—Microsoft, Yahoo, Google, Facebook, PalTalk, AOL, Skype, YouTube, and Apple.[11] The Director of National Intelligence has acknowledged the existence of the PRISM program but stated that it involves surveillance of foreigners outside the United States.[12] This is misleading. The PRISM program involves the collection of Americans' communications, both international and domestic, and for reasons explained below, the program is unconstitutional.

A. Section 702 is unconstitutional

President Bush signed the FISA Amendments Act into law on July 10, 2008.[13] While leaving FISA in place for purely domestic communications, the FISA Amendments Act revolutionized the FISA regime by permitting the mass acquisition, without individualized judicial oversight or supervision, of Americans' international communications. Under the FISA Amendments Act, the Attorney General and Director of National Intelligence ("DNI") can "authorize jointly, for a period of up to 1 year . . . the targeting of persons reasonably believed to be located outside the United States to acquire foreign intelligence information." 50 U.S.C. 1881a(a). The government is prohibited from "intentionally target[ing] any person known at the time of the acquisition to be located in the United States," *id*. § 1881a(b)(1), but an acquisition authorized under the FISA Amendments Act may nonetheless sweep up the international communications of U.S. citizens and residents.

Before authorizing surveillance under Section 702—or, in some circumstances, within seven days of authorizing such surveillance—the Attorney General and the DNI must submit to the FISA Court an application for an order (hereinafter, a "mass acquisition order"). *Id*. § 1881a(a), (c)(2). A mass acquisition order is a kind of blank check, which once obtained permits—without further judicial authorization—whatever surveillance the government may choose to engage in, within broadly drawn parameters, for a period of up to one year.

To obtain a mass acquisition order, the Attorney General and DNI must provide to the FISA Court "a written certification and any supporting affidavit" attesting that the FISA Court has approved, or that the government has submitted to the FISA Court for approval, "targeting procedures" reasonably designed to ensure that the acquisition is "limited to targeting persons

reasonably believed to be located outside the United States," and to "prevent the intentional acquisition of any communication as to which the sender and all intended recipients are known at the time of the acquisition to be located in the United States." *Id*. § 1881a(g)(2)(A)(i).

The certification and supporting affidavit must also attest that the FISA Court has approved, or that the government has submitted to the FISA Court for approval, "minimization procedures" that meet the requirements of 50 U.S.C. § 1801(h) or § 1821(4).

Finally, the certification and supporting affidavit must attest that the Attorney General has adopted "guidelines" to ensure compliance with the limitations set out in § 1881a(b); that the targeting procedures, minimization procedures, and guidelines are consistent with the Fourth Amendment; and that "a significant purpose of the acquisition is to obtain foreign intelligence information." *Id*. § 1881a(g)(2)(A)(iii)–(vii).

Importantly, Section 702 does not require the government to demonstrate to the FISA Court that its surveillance targets are foreign agents, engaged in criminal activity, or connected even remotely with terrorism. Indeed, the statute does not require the government to identify its surveillance targets at all. Moreover, the statute expressly provides that the government's certification is not required to identify the facilities, telephone lines, email addresses, places, premises, or property at which its surveillance will be directed. *Id*. § 1881a(g)(4).

Nor does Section 702 place meaningful limits on the government's retention, analysis, and dissemination of information that relates to U.S. citizens and residents. The Act requires the government to adopt "minimization procedures," *id*. § 1881a, that are "reasonably designed . . . to minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons," *id*. §§ 1801(h)(1), 1821(4)(A). The Act does not, however, prescribe specific minimization procedures. Moreover, the FISA Amendments Act specifically allows the government to retain and disseminate information—including information relating to U.S. citizens and residents—if the government concludes that it is "foreign intelligence information." *Id*. § 1881a(e) (referring to *id*. §§ 1801(h)(1), 1821(4)(A)). The phrase "foreign intelligence information" is defined broadly to include, among other things, all information concerning terrorism, national security, and foreign affairs. *Id*. § 1801(e).

As the FISA Court has itself acknowledged, its role in authorizing and supervising surveillance under the FISA Amendments Act is "narrowly circumscribed."[14] The judiciary's traditional role under the Fourth Amendment is to serve as a gatekeeper for particular acts of surveillance, but its role under the FISA Amendments Act is to issue advisory opinions blessing in advance broad parameters and targeting procedures, under which the government is then free to conduct surveillance for up to one year. Under Section 702, the FISA Court does not consider individualized and particularized surveillance applications, does not make individualized probable cause determinations, and does not closely supervise the implementation of the government's targeting or minimization procedures. In short, the role that the FISA Court plays under the FISA Amendments Act bears no resemblance to the role that it has traditionally played under FISA.

The ACLU has long expressed deep concerns about the lawfulness of the FISA Amendments Act and surveillance under Section 702.[15] The statute's defects include:

- Section 702 allows the government to collect Americans' international communications without requiring it to specify the people, facilities, places, premises, or property to be monitored

Until Congress enacted the FISA Amendments Act, FISA generally prohibited the government from conducting electronic surveillance without first obtaining an individualized and particularized order from the FISA court. In order to obtain a court order, the government was required to show that there was probable cause to believe that its surveillance target was an agent of a foreign government or terrorist group. It was also generally required to identify the facilities to be monitored. The FISA Amendments Act allows the government to conduct electronic surveillance without indicating to the FISA Court whom it intends to target or which facilities it intends to monitor, and without making any showing to the court—or even making an internal executive determination—that the target is a foreign agent or engaged in terrorism. The target could be a human rights activist, a media organization, a geographic region, or even a country. The government must assure the FISA Court that the targets are non-U.S. persons overseas, but in allowing the executive to target such persons overseas, Section 702 allows it to monitor communications between those targets and U.S. persons inside the United States. Moreover, because the FISA Amendments Act does not require the government to identify the specific targets and facilities to be surveilled, it permits the acquisition of these communications *en masse*. A single acquisition order may be used to justify the surveillance of communications implicating thousands or even millions of U.S. citizens and residents.

- Section 702 allows the government to conduct intrusive surveillance without meaningful judicial oversight.

Under Section 702, the government is authorized to conduct intrusive surveillance without meaningful judicial oversight. The FISA Court does not review individualized surveillance applications. It does not consider whether the government's surveillance is directed at agents of foreign powers or terrorist groups. It does not have the right to ask the government why it is initiating any particular surveillance program. The FISA Court's role is limited to reviewing the government's "targeting" and "minimization" procedures. And even with respect to the procedures, the FISA court's role is to review the procedures at the outset of any new surveillance program; it does not have the authority to supervise the implementation of those procedures over time.

- Section 702 places no meaningful limits on the government's retention and dissemination of information relating to U.S. citizens and residents.

As a result of the FISA Amendments Act, thousands

or even millions of U.S. citizens and residents will find their international telephone and email communications swept up in surveillance that is "targeted" at people abroad. Yet the law fails to place any meaningful limitations on the government's retention and dissemination of information that relates to U.S. persons. The law requires the government to adopt "minimization" procedures—procedures that are "reasonably designed . . . to minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons." However, these minimization procedures must accommodate the government's need "to obtain, produce, and disseminate foreign intelligence information." In other words, the government may retain or disseminate information about U.S. citizens and residents so long as the information is "foreign intelligence information." Because "foreign intelligence information" is defined broadly (as discussed below), this is an exception that swallows the rule.

- Section 702 does not limit government surveillance to communications relating to terrorism.

The Act allows the government to conduct dragnet surveillance if a significant purpose of the surveillance is to gather "foreign intelligence information." There are multiple problems with this. First, under the new law the "foreign intelligence" requirement applies to entire surveillance programs, not to individual intercepts. The result is that if a significant purpose of any particular government dragnet is to gather foreign intelligence information, the government can use that dragnet to collect all kinds of communications—not only those that relate to foreign intelligence. Second, the phrase "foreign intelligence information" has always been defined extremely broadly to include not only information about terrorism but also information about intelligence activities, the national defense, and even the "foreign affairs of the United States." Journalists, human rights researchers, academics, and attorneys routinely exchange information by telephone and email that relates to the foreign affairs of the U.S.

B. The NSA's "targeting" and "minimization" procedures do not mitigate the statute's constitutional deficiencies.

Since the FISA Amendments Act was enacted in 2008, the government's principal defense of the law has been that "targeting" and "minimization" procedures supply sufficient protection for Americans' privacy. Because the procedures were secret, the government's assertion was impossible to evaluate. Now that the procedures have been published, however,[16] it is plain that the assertion is false. Indeed, the procedures confirm what critics have long suspected—that the NSA is engaged in unconstitutional surveillance of Americans' communications, including their telephone calls and emails. The documents show that the NSA is conducting sweeping surveillance of Americans' international communications, that it is acquiring many purely domestic communications as well, and that the rules that supposedly protect Americans' privacy are weak and riddled with exceptions.

- The NSA's procedures permit it to monitor Americans' international communications in the course of surveillance targeted at foreigners abroad.

While the FISA Amendments Act authorizes the government to target foreigners abroad, not Americans, it permits the government to collect Americans' communications with those foreign targets. The recently disclosed procedures contemplate not only that the NSA will acquire Americans' international communications but that it will retain them and possibly disseminate them to other U.S. government agencies and foreign governments. Americans' communications that contain "foreign intelligence information" or evidence of a crime can be retained forever, and even communications that don't can be retained for as long as five years. Despite government officials' claims to the contrary, the NSA is building a growing database of Americans' international telephone calls and emails.

- The NSA's procedures allow the surveillance of Americans by failing to ensure that the its surveillance targets are in fact foreigners outside the United States.

The FISA Amendments Act is predicated on the theory that foreigners abroad have no right to privacy—or, at any rate, no right that the United States should respect. Because they have no right to privacy, the NSA sees no bar to the collection of their communications, including their communications with Americans. But even if one accepts this premise, the NSA's procedures fail to ensure that its surveillance targets are *in fact* foreigners outside the United States. This is because the procedures permit the NSA to *presume* that prospective surveillance targets are foreigners outside the United States absent specific information to the contrary—and to presume therefore that they are fair game for warrantless surveillance.

- The NSA's procedures permit the government to conduct surveillance that has no real connection to the government's foreign intelligence interests.

One of the fundamental problems with Section 702 is that it permits the government to conduct surveillance without probable cause or individualized suspicion. It permits the government to monitor people who are not even thought to be doing anything wrong, and to do so without particularized warrants or meaningful review by impartial judges. Government officials have placed heavy emphasis on the fact that the FISA Amendments Act allows the government to conduct surveillance only if one of its purposes is to gather "foreign intelligence information." As noted above, however, that term is defined very broadly to include not only information about terrorism but also information about intelligence activities, the national defense, and even "the foreign affairs of the United States." The NSA's procedures weaken the limitation further. Among the things the NSA examines to determine whether a particular email address or phone number will be used to exchange foreign intelligence information is whether it has been used in the past to communicate with foreigners. Another is whether it is listed in a foreigner's address book. In other words, the NSA appears to equate a propensity to communicate with foreigners with a propensity to communicate foreign intelligence information. The effect is to bring virtually every international

communication within the reach of the NSA's surveillance.

- The NSA's procedures permit the NSA to collect international communications, including Americans' international communications, in bulk.

On its face, Section 702 permits the NSA to conduct dragnet surveillance, not just surveillance of specific individuals. Officials who advocated for the FISA Amendments Act made clear that this was one of its principal purposes, and unsurprisingly, the procedures give effect to that design. While they require the government to identify a "target" outside the country, once the target has been identified the procedures permit the NSA to sweep up the communications of any foreigner who may be communicating "about" the target. The Procedures contemplate that the NSA will do this by "employ[ing] an Internet Protocol filter to ensure that the person from whom it seeks to obtain foreign intelligence information is located overseas," by "target[ing] Internet links that terminate in a foreign country," or by identifying "the country code of the telephone number." However the NSA does it, the result is the same: millions of communications may be swept up, Americans' international communications among them.

- The NSA's procedures allow the NSA to retain even purely domestic communications.

Given the permissive standards the NSA uses to determine whether prospective surveillance targets are foreigners abroad, errors are inevitable. Some of the communications the NSA collects under the Act, then, will be purely domestic.[17] The Act should require the NSA to purge these communications from its databases, but it does not. The procedures allow the government to keep and analyze even purely domestic communications if they contain significant foreign intelligence information, evidence of a crime, or encrypted information. Again, foreign intelligence information is defined exceedingly broadly.

- The NSA's procedures allow the government to collect and retain communications protected by the attorney-client privilege.

The procedures expressly contemplate that the NSA will collect attorney-client communications. In general, these communications receive no special protection—they can be acquired, retained, and disseminated like any other. Thus, if the NSA acquires the communications of lawyers representing individuals who have been charged before the military commissions at Guantanamo, nothing in the procedures would seem to prohibit the NSA from sharing the communications with military prosecutors. The procedures include a more restrictive rule for communications between attorneys and their clients who have been criminally indicted in the United States—the NSA may not share these communications with prosecutors. Even those communications, however, may be retained to the extent that they include foreign intelligence information.

C. Congress should amend Section 702 to prohibit suspicionless, dragnet collection of Americans' communications.

For the reasons discussed above, the ACLU believes that the FISA Amendments Act is unconstitutional on its face. There are many ways, however, that Congress could provide meaningful protection for privacy while preserving the statute's broad outline. One bill introduced by Senator Wyden during the reauthorization debate last fall would have prohibited the government from searching through information collected under the FISA Amendments Act for the communications of specific, known U.S. persons. Bills submitted during the debate leading up to the passage of the FISA Amendments Act in 2008 would have banned dragnet collection in the first instance or required the government to return to the FISC before searching communications obtained through the FISA Amendments Act for information about U.S. persons. Congress should examine these proposals again and make amendments to the Act that would provide greater protection for individual privacy and mitigate the chilling effect on rights protected by the First Amendment.

III. Excessive Secrecy Surrounds the Government's use of FISA authorities.

Amendments to FISA since 2001 have substantially expanded the government's surveillance authorities, but the public lacks crucial information about the way these authorities have been implemented. Rank-and-file members of Congress and the public have learned more about domestic surveillance in last two months than in the last several decades combined. While the Judiciary and Intelligence Committees have received some information in classified format, only members of the Senate Select Committee on Intelligence, party leadership, and a handful of Judiciary Committee members have staff with clearance high enough to access the information and advise their principals. Although the Inspectors General and others file regular reports with the Committees of jurisdiction, these reports do not include even basic information such how many Americans' communications are swept up in these programs, or how and when Americans' information is accessed and used.

Nor does the public have access to the FISC decisions that assess the meaning, scope, and constitutionality of the surveillance laws. Aggregate statistics alone would not allow the public to understand the reach of the government's surveillance powers; as we have seen with Section 215, one application may encompass millions of individual records. Public access to the FISA Court's substantive legal reasoning is essential. Without it, some of the government's most far-reaching policies will lack democratic legitimacy. Instead, the public will be dependent on the discretionary disclosures of executive branch officials—disclosures that have sometimes been self-serving and misleading in the past.[18] Needless to say, it may be impossible to release FISC opinions without redacting passages concerning the NSA's sources and methods. The release of redacted opinions, however, would be far better than the release of nothing at all.

Congress should require the release of FISC opinions concerning the scope, meaning, or constitutionality of FISA, including opinions relating to Section 215 and Section 702. Administration officials have said there are over a dozen such

opinions, some close to one hundred pages long.[19] Executive officials testified before Congress several years ago that declassification review was already underway,[20] and President Obama directed the DNI to revisit that process in the last few weeks. If the administration refuses to release these opinions, Congress should consider legislation compelling their release. Possible vehicles include the LIBERT-E Act, cited above, or the Ending Secret Law Act, H.R. 2475, 113th Cong. (2013), a bipartisan bill sponsored by Rep. Adam Schiff, Todd Rokita, and sixteen other members of the House.

Congress should also require the release of information about the type and volume of information that is obtained under dragnet surveillance programs. The leaked Verizon order confirms that the government is using Section 215 to collect telephony metadata about every phone call made by VBNS subscribers in the United States. That the government is using Section 215 for this purpose raises the question of what other "tangible things" the government may be collecting through similar dragnets. For reasons discussed above, the ACLU believes that these dragnets are unauthorized by the statute as well as unconstitutional. Whatever their legality, however, the public has a right to know, at least in general terms, what kinds of information the government is collecting about innocent Americans, and on what scale.

IV. Summary of Recommendations

As discussed above, the ACLU urges Congress to:

- Amend Section 215 of the Patriot Act and Section 702 of FISA to prohibit suspicionless, "dragnet" monitoring or tracking of Americans' communications.
- Require the publication of past and future FISC opinions insofar as they evaluate the meaning, scope, or constitutionality of the foreign-intelligence laws.
- Require the publication of information about the type and volume of information that the government obtains under dragnet surveillance programs.
- Hold additional hearings to consider further amendments to FISA—including amendments to make FISC proceedings more transparent.

Thank you for this opportunity to present the ACLU's views.

Endnotes

1 *See* Glenn Greenwald, *NSA Collecting Phone Records of Millions of Verizon Customers Daily*, Guardian, June 5, 2013, http://bit.ly/13jsdlb.

2 Secondary Order, *In Re Application of the FBI for an Order Requiring the Production of Tangible Things from Verizon Bus. Network Servs., Inc. on Behalf of MCI Commc'n Servs., Inc. d/b/a Verizon Bus. Servs.*, No. BR 13-80 at 2 (FISA Ct. Apr. 25, 2013), *available at* http://bit.ly/11FY393.

3 *See* Siobhan Gorman et al., *U.S. Collects Vast Data Trove*, Wall St. J., June 7, 2013, http://on.wsj.com/11uD0ue ("The arrangement with Verizon, AT&T and Sprint, the country's three largest phone companies means, that every time the majority of Americans makes a call, NSA gets a record of the location, the number called, the time of the call and the length of the conversation, according to people familiar with the matter. . . . AT&T has 107.3 million wireless customers and 31.2 million landline customers. Verizon has 98.9 million wireless customers and 22.2 million landline customers while Sprint has 55 million customers in total."); Siobhan Gorman & Jennifer Valentino-DeVries, *Government Is Tracking Verizon Customers' Records*, Wall St. J., June 6, 2013, http://on.wsj.com/13mLm7c.

In the days following *The Guardian*'s disclosure of the Verizon order, officials revealed other details about the government's surveillance under Section 215. *See* James R. Clapper, DNI Statement on Recent Unauthorized Disclosures of Classified Information, Office of the Director of National Intelligence (June 6, 2013), http://1.usa.gov/13jwuFc. The DNI stated, for example, that "the [FISC] only allows the data to be queried when there is a reasonable suspicion, based on specific facts, that the particular basis for the query is associated with a foreign terrorist organization."

4 Dan Roberts & Spencer Ackerman, *Senator Feinstein: NSA Phone Call Data Collection in Place 'Since 2006,'* Guardian, June 6, 2013, http://bit.ly/13rfxdu; *id.* (Senator Saxby Chambliss: "This has been going on for seven years.").

5 For ease of reference, this testimony uses "business records provision" to refer to the current version of the law as well as to earlier versions, even though the current version of the law allows the FBI to compel the production of much more than business records, as discussed below.

6 Records are presumptively relevant if they pertain to (1) a foreign power or an agent of a foreign power; (2) the activities of a suspected agent of a foreign power who is the subject of such authorized investigation; or (3) an individual in contact with, or known to, a suspected agent of a foreign power who is the subject of such authorized investigation. This relaxed standard is a significant departure from the original threshold, which, as noted above, required an individualized inquiry.

7 Jennifer Valentino-Devries & Siobhan Gorman, *Secret Court's Redefinition of 'Relevant' Empowered Vast NSA Data-Gathering*, Wall St. J., July 8, 2013, http://on.wsj.com/13x8QKU.

8 *See also Hale v. Henkel*, 201 U.S. 43, 76-77 (1906).

9 The metadata program also violates Section 215 because the statute does not authorize the prospective acquisition of business records. The text of the statute contemplates "release" of "tangible things" that can be "fairly identified," and "allow[s] a reasonable time" for providers to "assemble[]" those things. 50 U.S.C. § 1861(c)(1)-(2). These terms suggest that Section 215 reaches only business records already in existence.

10 Barton Gellman & Laura Poitras, *U.S., British Intelligence Mining Data From Nine U.S. Internet Companies in Broad Secret Program*, Wash. Post, June 7, 2013, http://wapo.st/1888aNr.

11 While news reports have generally described PRISM as an NSA "program," the publicly available documents leave open the possibility that PRISM is instead the name of the NSA database in which content collected from these providers is stored.

12 James R. Clapper, DNI Statement on Activities Authorized Under Section 702 of FISA, Office of the Director of National Intelligence (June 6, 2013), http://1.usa.gov/13JJdBE; *see also* James R. Clapper, DNI Statement on the Collection of Intelligence Pursuant to Section 702 of the Foreign Intelligence Surveillance Act (June 8, 2013), http://1.usa.gov/10YY4tp.

13 A description of electronic surveillance prior to the passage of the FISA Amendments Act, including the warrantless wiretapping program authorized by President Bush beginning in 2001, is available in Mr. Jaffer's earlier testimony to the Committee. *See* The FISA Amendments Act of 2008: Hearing Before the Subcomm. on Crime, Terrorism, and Homeland Security, H. Comm. on the Judiciary, 112th Cong. (May 31, 2012) (written testimony of Jameel Jaffer, Deputy Legal Director of the American Civil Liberties Union Foundation), *available at* http://bit.ly/14Q61Bs.

14 *In re Proceedings Required by § 702(i) of the FISA Amendments Act of 2008*, No. Misc. 08-01, slip op. at 3 (FISA Ct. Aug. 27, 2008) (internal quotation marks omitted), *available at* http://www.fas.org/irp/agency/doj/fisa/fisc082708.pdf.

15 The ACLU raised many of these defects in a constitutional challenge to the FISA Amendments Act filed just hours after the Act was signed into law

in 2008. The case, *Amnesty v. Clapper*, was filed on behalf of a broad coalition of attorneys and human rights, labor, legal and media organizations whose work requires them to engage in sensitive and sometimes privileged telephone and email communications with individuals located outside the United States. In a 5-4 ruling handed down on February 26, 2013, the Supreme Court held that the ACLU's plaintiffs did not have standing to challenge the constitutionality of the Act because they could not show, at the outset, that their communications had been monitored by the government. *See Clapper v. Amnesty Int'l USA*, 133 S. Ct. 1138 (2013). The Court did not reach the merits of plaintiffs' constitutional challenge.

16 *See* Glenn Greenwald & James Ball, *The Top Secret Rules that Allow NSA to Use US Data Without a Warrant*, *Guardian*, June 20, 2013, http://bit.ly/105qb9B.

17 Notably, a 2009 *New York Times* article discusses an episode in which the NSA used the Act to engage in "significant and systemic" overcollection of such domestic communications. Eric Lichtblau & James Risen, *Officials Say U.S. Wiretaps Exceeded Law*, N.Y. Times, April 15, 2009, http://nyti.ms/16AIq5O.

18 *See, e.g.*, Glenn Kessler, *James Clapper's 'Least Untruthful' Statement to the Senate*, Wash. Post, June 12, 2013, http://wapo.st/170VVSu.

19 *See* Eric Lichtblau, *In Secret, Court Vastly Broadens Powers of N.S.A.*, N.Y. Times, July 6, 2013, http://nyti.ms/12beiA3.

20 Prehearing Questions for Lisa O. Monaco Upon Her Nomination to be the Assistant Attorney General for National Security, Sen. Select Comm. on Intelligence, 112th Cong., at 12-13, *available at* http://bit.ly/10V5Ion.

First Principles: Are Judicial and Legislative Oversight of NSA Constitutional?

*Robert F. Turner**

This issue of *Engage* features a number of excellent essays about whether sensitive national security secrets leaked to the media disclose violations of the Constitution or of statutes like the Foreign Intelligence Surveillance Act (FISA). Based upon what I have read, I strongly believe that PRISM and the collection of metadata under Section 215 of the PATRIOT Act are lawful. But rather than repeating arguments already made by my friend Stewart Baker and other fine contributors, I want to address a more fundamental issue. Does Congress have the legal authority to regulate and/or demand secret information from the Executive about the collection of foreign intelligence information?

This is neither a frivolous question nor an issue of first impression for me. I worked as national security adviser to Senator Robert P. Griffin—the Assistant Minority Leader and a member of the Senate Foreign Relations Committee—when FISA was enacted in 1978, and it was my conclusion at the time that FISA was flagrantly unconstitutional. I've made the same point during congressional testimony[1] and elsewhere[2] since President George W. Bush's Terrorist Surveillance Program was first leaked by the *New York Times* in 2005.

I. The Original Constitutional Understanding on "The Business of Intelligence"

I begin with the observation that the Founding Fathers understood well that large deliberative bodies like Congress could not keep secrets well. When France in 1776 agreed to provide massive covert assistance to the American colonies, Benjamin Franklin and his four colleagues on the Committee of Secret Correspondence each signed a memorandum declaring that they had concluded they could not share the great news with others in the Second Continental Congress, because "We find by fatal experience that Congress consists of too many members to keep secrets."[3]

The Founding Fathers were remarkably well-read men, and they often quoted Locke, Montesquieu, and Blackstone—often called the "political bibles" of the Framers.[4] Each of these writers argued that, for reasons of institutional competency, the management of relations with the external world had to be left to the discretion of the Executive to be managed for the public good.

In his *Second Treatise on Civil Government*, John Locke explained in 1690 that the business of war and diplomacy had to be entrusted to the executive because legislative bodies could not keep secrets, act with speed or unity of plan, or anticipate in advance all of the changes that might occur during negotiations or on foreign battlefields. Paraphrasing Locke in explaining the new Constitution to the American people in 1788, John Jay wrote in *Federalist* No. 64 that "The loss of a battle, the death of a prince, the removal of a minister, or other circumstances intervening to change the present posture and aspect of affairs, may turn the most favorable tide into a course opposite to our wishes."

Emphasizing the need for secrecy in America's relations with the outside world, Jay wrote:

> There are cases where the most useful intelligence may be obtained, if the persons possessing it can be relieved from apprehensions of discovery. Those apprehensions will operate on those persons whether they are actuated by mercenary or friendly motives, and there doubtless are many of both descriptions, who would rely on the secrecy of the president, but who would not confide in that of the senate, and still less in that of a large popular assembly. The convention have done well therefore in so disposing of the power of making treaties, that although *the president* must in forming them act by the advice and consent of the senate, yet he *will be able to manage the business of intelligence in such manner as prudence may suggest*.

This need to protect secrets was also recognized by both houses of Congress in its legislation. Indeed, a look at early appropriations acts to fund diplomatic and intelligence activities reaffirms the view that "the business of intelligence" was confided in the discretion of the president. The boilerplate language used year after year read:

> [T]he President shall account specifically for all such expenditures of the said money *as in his judgment may be made public*, and also for the *amount* of such expenditures *as he may think it advisable not to specify*, and cause a regular statement and account thereof to be laid before Congress annually . . . ."[5]

Some read the constitutional text and wonder where this vast grant of presidential authority is hidden. There is no discussion of "foreign affairs," "diplomacy," or "foreign intelligence collection." The original understanding was that the control over what Locke called "war, peace, leagues and alliances" was encompassed in the "executive power" conveyed to the president in Article II, Section 1, of the Constitution.

As Thomas Jefferson explained in an April 1790 memorandum to President Washington:

> The Constitution . . . has declared that "the Executive power shall be vested in the President," submitting only special articles of it to a negative by the Senate. . . . *The transaction of business with foreign nations is executive altogether*; it belongs, then to the head of that department, except as to such portions of it as are specially submitted to the Senate. Exceptions are to be construed strictly.[6]

Washington shared Jefferson's memo with Representative James Madison and Chief Justice John Jay, and both agreed with Jefferson that—other than their negatives over treaties and nominations expressed in the Constitution—the Senate

Professor Turner holds both professional and academic doctorates from the University of Virginia School of Law, where in 1981 he co-founded the Center for National Security Law. He has served as chairman of both the ABA Standing Committee on Law and National Security and the National Security Law subcommittee of the Federalist Society's International and National Security Law practice group.

had "no constitutional right to interfere" with the business of diplomacy. As Washington explained, "all the rest being Executive and vested in the President by the Constitution."[7]

Jefferson's chief rival in Washington's cabinet, Alexander Hamilton, took the same position in his first *Pacificus* letter three years later, reasoning:

> [A]s the participation of the Senate in the making of treaties, and the power of the Legislature to declare war, are exceptions out of the general "executive power" vested in the President, they are to be construed strictly, and ought to be extended no further than is essential to their execution.[8]

The early constitutional practice was summarized in a February 19, 1804, note from President Jefferson to Treasury Secretary Albert Gallatin:

> The Constitution has made the Executive the organ for managing our intercourse with foreign nations. . . . The executive being thus charged with the foreign intercourse, no law has undertaken to prescribe its specific duties. . . . From the origin of the present government to this day . . . it has been the uniform opinion and practice that the whole foreign fund was placed by the Legislature on the footing of a contingent fund, in which they undertake no specifications, but leave the whole to the discretion of the President.[9]

II. Judicial Deference to the Executive

That same month, Chief Justice John Marshall—in perhaps the most famous Supreme Court decision of all times—reaffirmed that the Constitution grants the President important powers over foreign affairs that are checked neither by the Legislature nor the Judiciary:

> By the constitution of the United States, the President is invested with certain important political powers, in the exercise of which he is to use his own discretion, and is accountable only to his country in his political character, and to his own conscience . . . . The subjects are political. They respect the nation, not individual rights, and being intrusted to the executive, the decision of the executive is conclusive.
>
> The application of this remark will be perceived by adverting to the act of congress for establishing the department of foreign affairs. This officer, as his duties were prescribed by that act, is to conform precisely to the will of the president. . . . The acts of such an officer, as an officer, can never be examinable by the courts.[10]

In the 1936 *Curtiss-Wright* case, the Supreme Court noted that the President "makes treaties with the advice and consent of the Senate; but he alone negotiates. *Into the field of negotiation the Senate cannot intrude, and Congress itself is powerless to invade it.*"[11]

In this same landmark case, the Court noted:

> The marked difference between foreign affairs and domestic affairs in this respect is recognized by both houses of Congress in the very form of their requisitions for information from the executive departments. In the case of every department except the Department of State, the resolution directs the official to furnish the information. In the case of the State Department, dealing with foreign affairs, the President is requested to furnish the information "if not incompatible with the public interest." A statement that to furnish the information is not compatible with the public interest rarely, if ever, is questioned.[12]

Now, in candor, I believe the Court in *Curtiss-Wright* got the right answer for the wrong reasons. Justice Sutherland focused not upon the expressed grant of "executive power" to the President, but instead on the idea that the foreign policy power was a natural attribute of sovereignty that attached to the presidency at the time of America's independence from Great Britain. It was not an unreasonable explanation (and *Curtiss-Wright* remains by far the most often cited Supreme Court foreign affairs case), but it is clear that the Framers believed they had *expressly* vested this power in the President through Article II, Section 1's grant of "executive power."

This longstanding deference to presidential discretion in foreign affairs was recognized by both the courts and Congress into the second half of the twentieth century. In the 1953 case of *United States v. Reynolds*, the Supreme Court discussed the executive privilege to protect national security secrets, noting that: "Judicial Experience with the privilege which protects military and state secrets has been limited in this country . . . ." But the Court recognized an *absolute* privilege for military secrets, explaining:

> In each case, the showing of necessity [of disclosure] which is made will determine how far the court should probe in satisfying itself that the occasion for invoking the privilege is appropriate. Where there is a strong showing of necessity, the claim of privilege should not be lightly accepted, but *even the most compelling necessity cannot overcome the claim of privilege if the court is ultimately satisfied that military secrets are at stake*.[13]

Obviously, intelligence programs run by a Department of Defense agency (NSA) designed to intercept communications from our nation's enemies during a period of authorized war are among the most sensitive of "military secrets."

Four years later, Professor Edward S. Corwin, one of the nation's leading constitutional scholars of his era, wrote in his classic volume, *The President: Office and Powers*:

> So far as practice and weight of opinion can settle the meaning of the Constitution, it is today established that the President alone has the power to negotiate treaties with foreign governments; that he is free to ignore any advice tendered him by the Senate as to a negotiation; and that *he is final judge of what information he shall entrust to the Senate as to our relations with other governments*.[14]

In the 1959 *Barenblatt* case, the Supreme Court recognized that there are proper limits not only on the power of Congress to control Executive discretion, but even to "inquire" into matters vested by the people in the President: "Congress

. . . cannot inquire into matters which are within the exclusive province of one of the other branches of the Government. Lacking the judicial power given to the Judiciary, it cannot inquire into matters that are exclusively the concern of the Judiciary. Neither can it supplant the Executive in what exclusively belongs to the executive."[15]

III. The Congressional Assault on the Intelligence Community

Speaking at Cornell Law School in 1959, Senate Foreign Relations Committee Chairman J. William Fulbright captured the conventional wisdom shared by all three branches until that time when, in arguing for even greater presidential power, he explained:

> The pre-eminent *responsibility* of the President for the formulation and conduct of American foreign policy is clear and unalterable. He has, as Alexander Hamilton defined it, all powers in international affairs "which the Constitution does not vest elsewhere in clear terms." He possesses sole authority to communicate and negotiate with foreign powers. He controls the external aspects of the Nation's power, which can be moved by his will alone—the armed forces, the diplomatic corps, the Central Intelligence Agency, and all of the vast executive apparatus.[16]

This was the understanding of our Constitution until near the end of the Vietnam War, when an angry Congress began for the first time demanding classified secrets and set up House and Senate intelligence committees. President Nixon had been weakened by the Watergate scandal, and when he resigned he was replaced by Vice President Gerald Ford—who had never run for national office and thus had even less political strength to resist the encroaching Congress.

How did all of this happen? The earliest reference I have found proposing that Congress challenge presidential authority over foreign intelligence was in a 1969 book by radical activist Richard Barnet, a founder of the Institute for Policy Studies—alleged by some to have been a Soviet or Cuban front organization[17]—who wrote:

> Congressmen should demand far greater access to information than they now have, and should regard it as their responsibility to pass information on to their constituents. Secrecy should be constantly challenged in Congress, for it is used more often to protect reputations than vital interests. There should be a standing congressional committee to review the classification system and to monitor secret activities of the government such as the CIA.[18]

Revelations a few years later of abuses in the intelligence area set the stage for Barnet's dream to become a reality.

IV. Intelligence Committee "Abuses"

Were there in fact "abuses" involving the Intelligence Community? Anyone who followed the Church and Pike Committee hearings knows there were. But they were not, for the most part, acts of wrongdoing at the initiative of the Intelligence Community.

President Franklin D. Roosevelt bypassed his attorney general in 1936 and directly ordered J. Edgar Hoover to start "spying" on Americans thought possibly to be connected with communism or fascism. But Hoover had, on his own initiative, banned FBI "black bag" jobs nearly a decade before the Church Committee hearings took place.[19] Most of the abuses had already been investigated and made public by the attorney general before the hearings even began. And some of the sensationalized charges in the end turned out to be largely unfounded.

For example, most people who followed the hearings in the press came away with the idea that the CIA routinely went around "assassinating" foreign leaders who would not do what America demanded. In fact, when the Church Committee published its massive volume on the subject,[20] it admitted it had not found a *single* case in which the CIA had ever assassinated anyone. And Directors of Central Intelligence Richard Helms and William Colby had each issued orders that no one connected with the CIA would have anything to do with assassination long before the hearings began.[21]

What about Fidel Castro? Yes, at the instructions of Presidents Eisenhower and Kennedy the CIA did make several plots to dispatch the Cuban dictator with extreme prejudice. But given Castro's unlawful intervention in several Latin American countries, one might make a plausible case that a use of lethal force was permissible as an act of collective self-defense under Article 51 of the UN Charter. There was also a decision made to kill the Congo's Patrice Lumumba, but before any action was taken he was arrested by his own government and killed soon thereafter by rival leftist guerrillas after escaping from prison.[22] In all of the other cases investigated by the Committee, the CIA was cleared of wrongdoing.

When it was all over, even Senator Frank Church admitted that the CIA had not been a "rogue elephant" (as he had initially charged), and that virtually every activity on which he disapproved had been ordered by a president or senior policy official. His House counterpart, Representative Otis Pike, who chaired the House committee investigating CIA abuses, later declared:

> I wound up the hearings with a higher regard for the CIA than when I started. We did find evidence, upon evidence, upon evidence where the CIA said: "No, don't do it." The State Department or the White House said, "We're going to do it." The CIA was much more professional and had a far deeper reading on the down-the-road implications of some immediately popular act than the executive branch or administration officials. One thing I really disagreed with [Senator] Church on was his characterization of the CIA as a "rogue elephant." The CIA never did anything the White House didn't want. Sometimes they didn't want to do what they did.[23]

In 2009, the *Indiana Law Journal* published a legal analysis of recently declassified CIA documents that had been turned over to the Church and Pike committees in the mid-1970s and were referred to as the CIA "family jewels." The author of the article, a CIA attorney, examined each of the activities and concluded that all but one were lawful at the time they occurred. The exception—the involuntary exposure of U.S. citizens to LSD and other drugs—had been terminated during

the Kennedy administration more than a decade before the congressional investigations.[24]

On a more personal note, between 1981 and 1984 I served as Counsel to the President's Intelligence Board in the White House. As the senior White House attorney charged specifically with overseeing compliance with FISA, other statutes, and Executive Orders governing the Intelligence Community ("IC"), I worked with the general counsel and inspectors general of all of the departments and agencies in the IC. I came away from the experience with the deepest respect for the men and women who serve in the IC and their leaders.

Yes, there were violations, but most were inadvertent. For example, on one occasion the FBI had, pursuant to a FISA warrant, tapped the telephone of an East European embassy official known to be an intelligence operative. But when they came in Monday morning to listen to the tape, the FBI agents discovered that, while the foreign spymaster was out with his wife on Saturday night, the U.S. Person babysitter from down the street had used the tapped phone to chat at length with her boyfriend. The Bureau very carefully implemented the relevant Attorney General guidelines, protecting the privacy of the U.S. Persons involved and reporting the violation to my office.

There were rare instances of personal misconduct by IC employees, such as one individual who accessed a classified database to try to learn more about the man who was dating his former wife; but, across the board, such abuse was dealt with quickly and firmly—in this instance including termination of a military career a few years short of being eligible for retirement benefits.

Is there a possibility that NSA or other IC databases might be abused? Certainly there is, just as there is a possibility that medical or IRS records might be misused. But, as others in this issue have documented, the extensive oversight procedures—often including regular polygraph examinations in which employees are grilled about whether they have ever misused such resources—are probably greater than in any other area of government employment.

V. FISA was a Fraud

Like the War Powers Resolution,[25] the Foreign Intelligence Surveillance Act (FISA) was a constitutional fraud. In 1967, when in *Katz v. United States* the Supreme Court reversed its 1928 decision in *Olmstead v. United States* and held that telephone wiretaps were a "search or seizure" under the Fourth Amendment and thus required a warrant, the Court in footnote 23 was careful to exclude wiretaps involving "national security" from its holding.

The following year, when Congress enacted the first wiretap statute requiring a judicial warrant for wiretaps, the statute expressly recognized the president's constitutional power to authorize warrantless wiretaps for foreign intelligence purposes:

> Nothing contained in this chapter . . . shall limit the *constitutional power of the President* to take such measures as he deems necessary to protect the Nation against actual or potential attack or other hostile acts of a foreign power, *to obtain foreign intelligence information* deemed essential to the security of the United States, *or to protect national security information* against foreign intelligence activities.[26]

In 1972, a unanimous Supreme Court held in the *Keith*[27] case that when the government wishes to use a wiretap in a purely domestic national security case that does not involve foreign powers or their agents inside this country, a warrant would be required. However, the Court repeatedly emphasized that its holding did not constrain the president's warrantless use of wiretaps for national security cases involving foreign powers:

> We emphasize, before concluding this opinion, the scope of our decision. As stated at the outset, this case involves only the *domestic* aspects of national security. We have not addressed and express no opinion as to, the issues which may be involved with respect to *activities of foreign powers or their agents*.[28]

Noting that domestic national security surveillance might call for a different set of rules than existed for routine criminal warrants, the Court invited Congress to consider new legislation specifically addressing "domestic" national security wiretaps: "Given those potential distinctions between Title III criminal surveillances and those involving the *domestic* security, Congress may wish to consider protective standards for *the latter* which differ from those already prescribed for specified crimes in Title III."[29]

However, Senator Ted Kennedy responded by telling his colleagues that the Court had asked Congress to enact legislation requiring a judicial warrant for *foreign* intelligence collection, and thus was born the Foreign Intelligence Surveillance Act. Apparently, few members of Congress had paid much attention to the *Keith* case and thus followed Senator Kennedy's lead. President Carter also embraced the statute.

Attorney General Griffin Bell, however, was clearly concerned that Congress was usurping presidential power. In testimony before the House Permanent Select Committee on Intelligence, he stated:

> [T]he current bill recognizes no inherent power of the President to conduct electronic surveillance, and I want to interpolate here to say that *this does not take away the power of the President under the Constitution*. It simply, in my view, is not necessary to state that power, so there is no reason to reiterate or iterate it as the case may be. It is in the Constitution, whatever it is. *The President, by offering this legislation, is agreeing to follow the statutory procedure*.[30]

President Carter was certainly free to acquiesce in a usurpation of his constitutional powers, but he did not have the constitutional authority to deprive future presidents of their powers under the Constitution.

VI. The Fourth Amendment, the Judiciary, and the Foreign Intelligence Exception to the Warrant Requirement

I submit that there is nothing in the Constitution that empowers Congress to seize control of, as Locke put it, "the business of intelligence." The only arguable authority would be the Fourth Amendment, but that issue had been litigated

repeatedly and the courts had uniformly held that there was a foreign intelligence exception to the warrant requirement of the Fourth Amendment. During the Carter administration, for example, Attorney General Bell had authorized the surreptitious entry into the home of a suspected spy for Communist Vietnam (a permanent resident alien who had lived in the United States for more than a decade) by the name of Truong Dinh Hung. Truong's telephone was tapped, microphones were placed around his apartment, and a video camera was concealed in his place of work.

When Truong was arrested and charged with espionage, his lawyer sought to exclude all of the evidence obtained without a warrant. But the motion was rejected by both the district court and the Fourth Circuit Court of Appeals.

The Fourth Circuit noted that the Carter administration had "relied upon a 'foreign intelligence' exception to the Fourth Amendment's warrant requirement," contending that no warrant was necessary because of the President's "constitutional prerogatives in the area of foreign affairs."[31]

Relying upon *Keith* and applying a balancing test, the court provided a lengthy analysis of why the executive branch was better suited to decide these issues than federal judges and relied on *Curtiss-Wright* for the proposition that "separation of powers requires us to acknowledge the principal responsibility of the President for foreign affairs and concomitantly for foreign intelligence surveillance."[32] It emphasized that this "foreign intelligence exception to the warrant requirement" was only applicable to cases involving "a foreign power, its agent or collaborators."[33]

When Congress enacted FISA in 1978, it created an appellate court (the FISA Court of Review) to consider appeals from the lower court charged with considering applications for foreign intelligence electronic surveillance warrants. In 2002, the Court of Review declared in a unanimous opinion:

> The *Truong* court, as did all the other courts to have decided the issue, held that the President did have inherent authority to conduct warrantless searches to obtain foreign intelligence information. . . . *We take for granted that the President does have that authority and, assuming that is so, FISA could not encroach on the President's constitutional power*.[34]

The Supreme Court has never decided a case involving the constitutionality of FISA. At least five pre-FISA cases were appealed to the Court, but *cert* was never granted. Some may see this as evidence that the issue is unsettled. I would suggest to the contrary. Surely, if the justices believed that the president lacked the constitutional authority to collect foreign intelligence information by warrantless electronic surveillance, they would have voted to grant cert and strike down the convictions. But the Court routinely denies *cert* to cases where all of the circuits are in agreement and the court believes they have decided the issues correctly.

For example, the Supreme Court has never formally decided that warrantless searches by federal Transportation Security Administration (TSA) officers of the persons and baggage of passengers on commercial airlines are lawful. It has made favorable references to the practice in dicta in other cases, but since the circuits are in agreement there has been no need for the Supreme Court to formally consider the issue.

Consider this excerpt from the Court's opinion in the 1989 case of *National Treasury Employees Union v. Von Raab:*

> While we have often emphasized, and reiterate today, that a search must be supported, as a general matter, by a warrant issued upon probable cause, . . . our decision in *Railway Labor Executives* reaffirms the longstanding principle that neither a warrant nor probable cause, nor, indeed, any measure of individualized suspicion, is an indispensable component of reasonableness in every circumstance. . . . As we note in *Railway Labor Executives,* our cases establish that where a Fourth Amendment intrusion serves special governmental needs, beyond the normal need for law enforcement, it is necessary to balance the individual's privacy expectations against the Government's interests to determine whether it is impractical to require a warrant or some level of individualized suspicion in the particular context.[35]

Indeed, in *Von Raab*, the Supreme Court noted that all of "the lower courts that have considered the question have consistently concluded that such [airport] searches are reasonable under the Fourth Amendment." The Court then quoted analysis from a leading case (*Edwards*) upholding warrantless airport searches: "When the risk is the jeopardy to hundreds of human lives and millions of dollars of property inherent in the pirating or blowing up of a large airplane, that danger alone meets the test of reasonableness . . . ."

Surely, stopping the next 9/11 attack is as important as preventing the hijacking of a commercial airliner. And just as surely, the Constitution entrusts "the business of intelligence" to the discretion of the president. Both Congress and the courts have recognized that there is a constitutional power invested in the president to engage in warrantless electronic surveillance to protect the nation from foreign powers (a term that includes foreign terrorist organizations like al Qaeda) and their agents within our own borders.

VII. The Harm Caused by FISA

Sadly, the unconstitutional FISA statute has done serious harm to our nation. Reaffirming the wisdom of Locke's observation that legislative assemblies cannot anticipate everything that might take place in negotiations or on a battlefield, when Congress enacted FISA it made it a felony for NSA, the FBI, or any other U.S. government authority to obtain a FISA warrant based upon any activity that is protected by the First Amendment. No doubt they were intending to immunize Jane Fonda's actions during the Vietnam War.[36] But they didn't anticipate the possibility that we might be attacked by religious extremists who would kill thousands of our fellow Americans. Under FISA, if a religious extremist writes an op-ed article or gives a speech declaring that Allah wants all Infidels killed and that is the duty of every Muslim, our Intelligence Community cannot use that information to seek a FISA warrant.

Another threat Congress failed to anticipate was the

"lone wolf" terrorist like Zacharias Moussaoui. The FBI identified Moussaoui as a probable terrorist weeks before the 9/11 attacks, and much earlier became suspicious of two of the terrorists who flew the plane into the Pentagon on that tragic day. But thanks to FISA, they were not allowed to engage in the kinds of surveillance that might have uncovered and prevented the 9/11 attacks because they could not tie the suspects to a "foreign power."

So, rather than worrying about whether ongoing NSA programs are consistent with FISA (and, for the record, they are), someone ought to be asking whether FISA is consistent with the U.S. Constitution.

Endnotes

1 *See, e.g., Congress, Too, Must 'Obey the Law: Why FISA Must Yield to the President's Independent Constitutional Power to Authorize the Collection of Foreign Intelligence: Hearing on "Wartime Executive Power and the NSA's Surveillance Authority II" Before the S. Comm. on Judiciary,* 109th Cong. 2 (2006) (statement of Robert F. Turner, Prof. of Law, Univ. of Virginia School of Law), *available at* http://www.virginia.edu/cnsl/pdf/TURNER-SJC-28Feb06%20FINAL.pdf; *Is Congress the Real "Lawbreaker"?: Reconciling FISA with the Constitution: Hearing on "Warrantless Surveillance and the Foreign Intelligence Surveillance Act: The Role of Checks and Balances in Protecting Americans' Privacy Rights" Before the H. Judiciary Comm.*, 110th Cong. 1 (2007) (statement of Robert F. Turner, Prof. of Law, Univ. of Virginia School of Law), available at http://www.virginia.edu/cnsl/pdf/Turner-HJC-5Sept07-(final).pdf.

2 *FISA vs. the Constitution: Congress can't usurp the president's power to spy on America's enemies*, Wall. St. J., Dec. 28 2005, http://www.opinionjournal.com/editorial/feature.html?id=110007734.

3 Verbal statement of Thomas Story to the Committee, 2 Paul Force, American Archives: A Documentary History of the North American Colonies, 5th Ser., 819 (1837-53).

4 *See, e.g.,* Quincy Wright, The Control of American Foreign Relations 363 (1922).

5 *See, e.g.*, 1 Stat. 129 (1790) (emphasis added).

6 *Jefferson's Opinion on the powers of the Senate Respecting Diplomatic Appointments,* April 24, 1790, in 3 Writings of Thomas Jefferson 16 (Mem. ed. 1903) (emphasis added).

7 4 Diaries of George Washington 122 (Regents' Ed. 1925).

8 15 The Papers of Alexander Hamilton 39 (Harold C. Syrett ed., 1969).

9 *Jefferson to Gallatin,* 11 Writings of Thomas Jefferson, 5, 9, 10 (Mem. ed. 1903).

10 Marbury v. Madison, 5 U.S. (1 Cranch) 137, 165 (1803).

11 United States v. Curtiss-Wright Export Corp., 299 U.S. 304, 319 (1936) (emphasis added).

12 *Id.* at. 319-21 (emphasis added).

13 United States v. Reynolds, 345 U.S. 1, 11 (1953).

14 Edward S. Corwin, The President: Office and Powers 211-12 (4th rev. ed. 1957) (emphasis added).

15 Barenblatt v. United States, 360 U.S. 109 (1959).

16 The Federalist No. 64, at 434-35 (John Jay) (Jacob E. Cooke ed. 1961) (emphasis added).

17 *See, e.g.,* S. Steven Powell, Covert Cadre: Inside the Institute for Policy Studies 359 (1987); Ladislav Bittman The KGB and Soviet Disinformation: An Insider's View (1985). Writing in *National Review* in 1978, Brian Crozier, the director of the London Institute for the Study of Conflict, described the Institute for Policy Studies as the "perfect intellectual front for Soviet activities which would be resisted if they were to originate openly from the KGB.

18 Richard J. Barnet, The Economy of Death 178-79 (1969).

19 2 Sen. Rep't No. 94-755 at 24 (1976); 3 *id.* at 355.

20 Alleged Assassination Plots Involving Foreign Leaders, S. Rep't. No. 94-465 (1975).

21 *See* Robert F. Turner, *It's Not Really "Assassination" Legal and Moral Implications of Intentionally Targeting Terrorists and Aggressor-State Regime Elites*, 37 U. Rich. L. Rev. 791- 98 (2003).

22 S. Rep't. No. 94-465 at 256.

23 Frank J. Smist, Jr., Congress Oversees the United States Intelligence Community 197 (1990).

24 Daniel L. Pines, *The Central Intelligence Agency's "Family Jewels: Legal Then? Legal Now?,* 84 Ind. L. J. 637 (2009), *available at* http://www.repository.law.indiana.edu/cgi/viewcontent.cgi?article=1108&context=ilj.

25 *See, e.g.*, Robert F. Turner, The War Powers Resolution: Its Implementation in Theory and Practice (1983); Robert F. Turner, Repealing the War Powers Resolution: Restoring the Rule of Law in U.S. Foreign Policy (1991).

26 18 U.S.C. § 2511(3) (1970) (emphasis added).

27 United States v. United States District Court, 407 U.S. 297(1972). The case is commonly referred to as the "*Keith* Case" because it was decided by Judge Damon Keith of the Eastern District of Michigan.

28 407 U.S. at 308, 321-22 (emphasis added).

29 407 U.S. at 322-23 (emphasis added).

30 Testimony of Attorney General Griffin Bell, Foreign Intelligence Electronic Surveillance, Hearings Before the Subcommittee on Legislation of the Permanent Select Committee on Intelligence, House of Representatives, January 10, 1978 at 14-15 (emphasis added).

31 United States v. Truong, 629 F.2d 908, 912 (1980).

32 *Id.* at 914 (1980).

33 *Id.* at 912, 915.

34 *In re Sealed Case*, 310 F.3d 717, 742 Foreign Int. Surv. Ct. Rev., Nov. 18, 2002 (No. 02-002, 02- 001).

35 National Treasury Employees Union v. Von Raab, 489 U.S. 656 at 665-66 (1989).

36 This is not the time for a lengthy discussion of Jane Fonda's conduct during her visit to Hanoi in August 1972, but she made broadcasts to American sailors on "Radio Hanoi" in which she urged them to refuse to obey orders and alleged that the bombs they were being asked to load on aircraft were actually filled with illegal poison chemicals, noting that following World War II war criminals were put to death.

Slouching Toward Mordor

*Grover Joseph Rees**

I sometimes visit a country whose government pervasively monitors the communications of its citizens, residents, and visitors. I am reluctant to name this country because representatives of its government may also be monitoring this publication, so I'll call it the Democratic Republic of Mordor.

When I am in Mordor I am careful never to communicate with anyone about politics, religion, or anything else the government might consider subversive. But this is not enough to avoid getting into trouble: before each trip I must also ask all my friends in the United States and elsewhere who might communicate with me by phone or email to avoid any discussion of politics, and particularly of words such as "freedom", "human rights", and "democracy." And if my friends work for organizations that have such words in their names—or for other entities that might be considered suspicious, such as the United States Government—I ask them not to communicate with me at all. The reason I take these steps is that I am reliably informed that while the government of Mordor systematically scans all electronic communications, it is logistically constrained to be far more selective about whose communications it actually reads or listens to. And the way to stay off that list is to avoid red flags such as talking about democracy or receiving a message from someone at Freedom House.

So I had seriously mixed feelings when I learned about the scope of our own government's collection of communications records. Like most Americans, I consider myself a strong supporter of the war on terror. I believe that Bradley Manning and Edward Snowden committed crimes for which they ought to receive just punishment. As a government official for 25 years I had frequent occasion to complain that we classified way too much information, but it never occurred to me that the remedy was to violate my oath of office by unilaterally declassifying whatever information I thought should be made public. I also agree with my friend Stewart Baker that gathering intelligence about terrorism "isn't patty cake." I have therefore been generally supportive of Section 215 of the Patriot Act, which gives the government authority to seize records in the hands of telephone companies and other third parties—but only after proving to a special court that the records in question are relevant to an investigation to obtain foreign intelligence information or to protect against terrorism or espionage.

My support was based in part on my confidence that the court would require the government to present evidence that the records in question were genuinely relevant to a specific investigation. This confidence was bolstered a few months ago when the Director of National Intelligence, testifying before Congress, categorically denied that the NSA had collected "any type of data at all on millions of Americans."

So I was stunned to learn that the NSA, with the court's approval, had secretly collected the records of *all* the calls of *all* the subscribers of the major telephone companies in the United States and assembled similar collections of email messages, Facebook postings, and other internet communications. Notwithstanding the subsequent reassurances that NSA will never actually listen to my calls or read my emails unless they have reason to believe I have been communicating with terrorists, I find it disturbing that they have collected and are keeping this information.

My reaction stems in part—but only in part—from a visceral distaste for big government. Like many conservatives, I have always opposed the idea of a national identification card, notwithstanding how useful it might be to immigration enforcement and other important objectives. For that matter, many of us are still unhappy that the government broke its promise that Social Security numbers would never be used for anything but keeping track of our Social Security accounts. And most Americas are glad we have drones to spy on Al Qaeda and the Taliban, but we don't want them spying on us.

The argument that we shouldn't be worried if we have nothing to hide misses the point. Conservatives and others oppose intrusive government not so much because of specific things we are afraid the government will discover as because they make the government of the United States look and feel too much like the government of Mordor. We know our government's objectives are mostly noble, while the objectives of dictatorships are frequently ignoble. But the objectives of such governments are not the only thing—indeed, not even the main thing—we find distasteful. The worst thing about them is their methods.

Nor is it clear that these new domestic intelligence gathering powers will not be abused—or, even more likely, expanded even further to include activities that would now be widely regarded as abusive but that will gradually come to be seen as the new normal.

My own experience in government, as an executive branch lawyer and policy-maker and also as a legislative branch employee attempting to exercise oversight, makes me skeptical of the argument that the government will collect and keep this metadata but hardly ever use it. My government experience was not in agencies whose primary function was intelligence gathering. But in parallel situations—in decision making processes on such matters as the official use of firearms by agency employees, the forced repatriation of asylum seekers to dangerous places, and whether the United States should support a United Nations appointment for a foreign government official who was credibly accused of mass murder—the institutional culture of executive branch decision making bodies was to push all the envelopes as far as they could be pushed in order to resolve the crisis at hand. Arguments along the lines of "Americans don't do things like this" did not resonate at all in these meetings. Related arguments, such as "we have to consider the optics," were occasionally successful in smoothing some of the roughest edges of proposed policies, but voices

.....

Grover Joseph Rees is a former law professor, judge, and ambassador. Some of the thoughts expressed in this article are based on his essay in The Treaty Power (symposium with A. Sofaer, H. Koh, and J. Nowak), 43 U. Miami L. Rev. 101 (1988).

of moderation were generally dismissed as "unhelpful" and sometimes the proponents of these arguments were not invited to the next meeting. When employees of NSA or another agency encounter a problem whose solution they believe might be advanced by more ambitious uses of the collected phone and email records—and assuming that the FISA court does not change its self-described practice of pretty much trusting the government to police itself—I can think of nothing that would make the dynamics of the decision making process any less goal-driven than such processes usually are.

One form this expansion could take would be with respect to how many degrees of separation should be required between you and the terrorist before you become a person of interest. If I interpret correctly the statements of those who defend the NSA metadata collection practices, the several hundred cases in which these data have been used to identify and monitor the substance of communications have involved people who received calls or messages directly from suspected terrorists. But surely it might also be useful to know more about the communications of people who regularly call people who are in touch with terrorists. And what about people whose communication links, either direct or attenuated, are not with suspected terrorists but with leakers such as Snowden and Manning? Or with people who are suspected of facilitating the leaks? After only three or four iterations of any of these moves, the NSA could be listening to an awful lot of innocent people. Most of us don't know much about who calls the people who call us, but few of us would want to be held accountable for the things that are posted by the friends of our Facebook friends.

This is not to say that the current NSA metadata collection practices can never be justified, but only that they need a stronger justification than has been offered so far. In particular, are there less intrusive methods that would serve the program's objectives as well or almost as well? Although some proponents of the current program argue that the data will disappear if not collected by the government, it appears that the Drug Enforcement Agency has been collecting similar information from AT&T on a case-by-case basis and that the company does maintain the records for long enough to suit DEA's purposes.

Perhaps there is some reason that seizing communications records only of persons who appear to have received calls or messages from terrorists would not work. If so, this reason should be clearly articulated and thoroughly debated.

Some legal scholars would argue that the proper place for the debate on whose records will be seized is within the NSA and other agencies of the executive branch. According to these scholars, if the President determines that such seizures will be helpful in the conduct of the war on terror, Congress has no constitutional authority to limit executive action pursuant to this determination.

This view of executive power over foreign affairs, and particularly over the conduct of declared and undeclared wars, finds strong support in the Supreme Court's decision in *United States v. Curtiss-Wright Export Corp.*,[1] which spoke of "the very delicate, plenary, and exclusive power of the President as the sole organ of the federal government in the field of international relations." The President's "sole organ" power, according to the Court in *Curtiss-Wright*, exists apart from the specific executive authorities enumerated in the Constitution. Rather, it consists of certain "attributes of sovereignty" that the Court regarded as implicit in the concept of nationhood. Later defenders of the "sole organ" power have sought to ground it in the text of the Constitution—principally in the designation of the President as Commander-in-Chief of the armed forces and in what they believe to be the plain meaning of the words "the executive power"—and in statements by some of the Framers. But the *Curtiss-Wright* Court was emphatic that the power was prior to and independent of the Constitution, having been derived from "the external powers passed from the Crown."

My own view is that the *Curtiss-Wright* doctrine is essentially anti-constitutional. Its central assumption is that the scope and allocation of foreign affairs powers in the government of the United States cannot have been intended to be fundamentally different than those of other governments. This amounts to a denial of the central theme of our Constitution: the limitation and distribution of sovereignty, often in ways that King George and Metternich would have regarded as unthinkable.

Especially when the executive action in question is directed at activities of United States citizens within the United States, a more appropriate analysis of legislative and executive authority is the one set forth in Justice Jackson's concurrence in the *Steel Seizure*[2] case: only when the President acts with the "express or implied authorization of Congress . . . may he be said (for what it may be worth) to personify the federal sovereignty." When, however, the President "takes measures incompatible with the expressed or implied will of Congress, his power is at its lowest ebb . . . .Presidential claim to a power at once so conclusive and preclusive must be scrutinized with caution, for what is at stake is the equilibrium established by our constitutional system."[3]

In the current controversy over metadata collection the executive branch, whatever reservations some of its officials may harbor about Congressional authority to limit domestic intelligence gathering, appears to have observed the procedures prescribed by Congress in Section 215 and related statutory provisions and to have relied on the substantive standards set forth in these provisions. It therefore seems appropriate for Congress to consider whether the collection of all telephone, email, and social media records—well in advance of any particular investigation but in anticipation of the possibility of such an investigation—is consistent with the relevancy standard it thought it was enacting in Section 215. If not, Congress should clarify the standard.

Other proposed safeguards, such as declassifying FISA court judgments or making their proceedings adversarial by including a public advocate—an attorney who might or might not be a government official, and who would be charged with defending the rights not of terrorists but of innocent bystanders—should also be considered but would be of limited use if the legal standard for relevancy is as broad as the NSA and the FISA court have construed it to be. Another interesting proposal, for criminal and/or employment-based penalties against federal employees and contractors who abuse collected

information, would provide significant protection only if it were not limited to abuse whose motives were extraneous to the employee's official duties. Although the collection and analysis of secret information on lovers and rivals—a type of surveillance known in the intelligence community as LOVEINT—is indeed abusive, the privacy of most Americans is far more likely to be violated by overzealous federal agents who sincerely but erroneously believe they are doing their jobs.

Most Americans recognize and accept the need to sacrifice some of their privacy in the interest of security, and most will surely acquiesce in the loss of yet another chunk of their privacy if it can be proved to their satisfaction that the collection of all their phone and internet communications records is essential to the prevention of terrorism. Such acquiescence is less likely if the showing is only that the government entities that specialize in the collection of such records have decided it would be more convenient to collect everyone's records in advance, just in case they should ever come in handy.

Endnotes

1 299 U.S. 304 (1936).

2 Youngstown Sheet & Tube Co. v. Sawyer, 343 U.S. 579 (1952).

3 *Id.* at 634-55.