**Testimony of Professor David Cole**

**Georgetown University Law Center**

**Before the Judiciary Committee of the United States House of Representatives**

**"Recommendations to Reform Foreign Intelligence Programs"**

**February 4, 2014**

## INTRODUCTION

Chairman Goodlatte, Ranking Member Conyers, and members of the Committee, I appreciate the opportunity to testify today on proposals to reform foreign intelligence gathering.[1] Since June 2013, the American public, and the world at large, have learned of a dizzying array of previously secret surveillance activities carried out by the National Security Agency (NSA) – some of them authorized by Congress, many of them apparently carried out exclusively under Executive Order 12333. Whatever one thinks of Edward Snowden's acts in revealing these programs, one thing is beyond dispute: the disclosures have touched off the most significant debate on the appropriate limits of surveillance this country – and possibly the world at large – has ever before undertaken.

While these programs remained secret, they were maintained by the executive branch, approved by the judiciary, and reauthorized (albeit in most cases, unknowingly) by Congress. Now that the programs have become public, all three branches of government have begun to reassess what they previously tolerated as long as they remained secret. President Obama appointed an expert Review Group to study the issue, and that Review Group, which featured the former counterterrorism adviser to the National Security Council and the former acting director of the CIA, recommended 46 reforms to rein in the NSA and increase transparency, accountability, and ultimately, trust among the American people and the world at large.[2] The President himself delivered a national speech last month on the subject, and adopted some of his Review Group's recommendations.

The Privacy and Civil Liberties Oversight Board has issued its own substantial report, focused on the Section 215 telephone records program and the Foreign Intelligence Surveillance Court, and has urged termination of the bulk collection of metadata.[3] Notably, the Privacy Board examined classified evidence and held classified briefings on the effectiveness of the program,

[1] I am a professor at Georgetown University Law Center, but appear before you today in my personal capacity.
[2] Liberty and Security in a Changing World, Report and Recommendations of The President's Review Group on Intelligence and Communications Technologies (hereinafter "Review Group Report"), Dec. 12, 2013, available at http://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf.
[3] Privacy and Civil Liberties Oversight Board, Report on the Telephone Records Program Conducted under Section 215 of the USA PATRIOT Act and on the Operations of the Foreign Intelligence Surveillance Court (hereinafter "Privacy Board Report"), Jan. 23, 2014, available at http://www.pclob.gov/SiteAssets/Pages/default/PCLOB-Report-on-the-Telephone-Records-Program.pdf.

and concluded that its security benefits have been, in seven years, marginal at best. It found that the program has not led to the disruption of any act or attempted act of terrorism. The only instance in which the Section 215 phone records program has led to the discovery of a single otherwise unknown person charged with a terrorist crime involved an attempt to send money to Al Shabaab, a Somalian organization, in violation of prohibitions on material support to that group. The Privacy Board recommends termination of the bulk phone records collection, because it finds that it was not authorized by statute in the first place, and because the risks it poses to privacy outweigh the benefits to security that it has provided.[4]

The courts have also begun to question the program. Judge Richard Leon of the U.S. District Court for the District of Columbia, has ruled that the program is likely unconstitutional.[5] Judge William Pauley of the Southern District of New York has reached an opposite conclusion.[6] Both cases are pending on appeal. Remarkably, the Foreign Intelligence Surveillance Court (FISC) itself issued no opinion on the lawfulness of the program when it initially authorized the program in May 2006. Nor did the FISC address the legality of the bulk metadata program on any of the subsequent occasions when, every 90 days, it reauthorized the program. In fact, the FISC did not write an opinion explaining its rationale until August 2013, many years after it had approved the program, and not coincidentally, two months after Edward Snowden disclosed the existence of the program.

Congress, meanwhile, is considering multiple bills proposing to rein in aspects of the NSA program. I support the bill introduced by Representative Jim Sensenbrenner and Senator Pat Leahy, the USA Freedom Act. It would make many changes, but among the most important is an amendment of Section 215 of the USA Patriot Act to require that the government show some nexus between the business records it seeks and a person or persons properly targeted for a foreign intelligence investigation. This would permit the NSA to obtain data related to suspects, but would not permit it to engage in bulk collection of every American's business records. The bill would restore an approach to privacy that has governed in this country since its founding – namely, the notion that the government should only invade privacy where it has some individualized objective basis for suspicion. It would end the dragnet collection of records about ordinary, law-abiding Americans who have no connection to terrorism, while retaining the ability of the government to gather information on those it has reason to believe are so connected.

The above activity by the three branches of government is in turn a reflection of the widespread public concern that has been expressed about the NSA's activities, both at home and abroad. For the first time since many of these programs' secret inception, the American people, and indeed the world at large, have had the opportunity to consider whether the NSA's activities accord with our most fundamental values of privacy, liberty, and equality. The last seven months of revelations have demonstrated that technology has advanced far beyond the law,

[4] Two members of the Privacy Board dissented from this recommendation.
[5] *Klayman v. Obama*, 2013 U.S. Dist. LEXIS 176925 (D.D.C. Dec. 16, 2013).
[6] *ACLU v. Clapper*, 2013 U.S. Dist. LEXIS 180863 (S.D.N.Y. Dec. 27, 2013).

affording the government the ability to construct detailed portraits of the most intimate associations, beliefs, and desires of any of us. Perhaps understandably, the NSA has sought to exploit these capabilities as aggressively as possible. After all, its mandate is to gather intelligence, not to balance security and privacy.

But the revelations also demonstrate that unless the law is adapted to catch up to technological change, we are at risk of forfeiting our privacy by default. This truth has been recognized by President Obama in his NSA speech, by his expert Review Group, and by the Privacy and Civil Liberties Oversight Board. It's been recognized by scholars across the country. And it's been recognized, in different contexts, by most members of the Supreme Court. Just as privacy laws had to adapt to the invention of the automobile, the telephone, the beeper, the GPS, and the thermal imaging device, so, too, they need to adapt to the government's increasing ability to use computers to collect and analyze massive amounts of digital data about all of us.

Congress has a critical role to play in adjusting the law to reflect the challenges of technology. As Justice Samuel Alito noted in the Supreme Court's most recent foray into this area, *United States v. Jones*, 132 S. Ct. 945, 964 (2012), "a legislative body is well situated to gauge changing public attitudes, to draw detailed lines, and to balance privacy and public safety in a comprehensive way." Unlike a court, Congress can consider the problem from a broader perspective. Congress can respond more quickly than the courts. And Congress may have a better sense of the privacy demands of the American people. Thus, Congress has in the past often responded to Supreme Court decisions that did not extend Fourth Amendment protection to particular forms of investigation by imposing statutory limits that protect the American people's privacy.

My testimony will focus the NSA's telephone records program, and will consist of three parts. First, I will underscore the substantial privacy concerns raised by bulk collection of digital data, and show why current legal limits are insufficient to preserve privacy. Second, I will discuss the importance of a Congressional response. And third, I will state why I think the Sensenbrenner-Leahy bill is a fitting response to the current situation.

## I. THE PRIVACY AND ASSOCIATIONAL ISSUES AT STAKE

As President Obama, his expert Review Group, and the Privacy and Civil Liberties Oversight Board all agreed, technology in the digital age poses significant risks to the privacy that all of us hold dear. The Constitution's framers, recognizing that privacy is the lifeblood of democracy, enacted the Fourth Amendment to prohibit general warrants and unreasonable searches and seizures. It is no less true today that privacy is essential to a functioning democracy and a healthy community. Now, as then, privacy is critical for the intimacy that is necessary to human flourishing. Now, as then, privacy affords the breathing room necessary for those who dissent

from the majority to gather together, express their views, and engage in political activity. As George Orwell and Ray Bradbury have shown, a society without privacy is associated with totalitarianism, and is not one in which any of us would want to live.

But if privacy is no less essential today than it was at the time of the Constitution's framing, it is much less secure. If, at the time of the framing, the government wanted to know what an individual in the privacy of his home read and wrote, and with whom he associated, it would have to obtain a warrant to search his home. Even with a warrant, the government generally had no way of knowing an individual's innermost beliefs or desires.

Today, by contrast, without a warrant or individualized suspicion, the government can learn what one reads, writes, with whom one associates, and even what one desires, simply by collecting "business records" – the records of internet service providers, phone companies, banks, credit card companies, libraries, and the like. In the modern age, nearly everything we do leaves a digital trace. As the President's expert Review Group noted, quoting the National Academy of Sciences, the "essence of the information age," is that everyone leaves "personal digital tracks … whenever he or she makes a purchase, takes a trip, uses a bank account, makes a phone call, walks past a security camera, obtains a prescription, sends or receives a package, files income tax forms, applies for a loan, e-mails a friend, sends a fax, rents a video, or engages in just about any other activity."[7]

President Obama similarly noted the ability of computers to obtain such information, and the privacy concerns that capability raises. As he stated,

> Corporations of all shapes and sizes track what you buy, store and analyze our data, and use it for commercial purposes; that's how those targeted ads pop up on your computer or smartphone. But all of us understand that the standards for government surveillance must be higher. Given the unique power of the state, it is not enough for leaders to say: trust us, we won't abuse the data we collect. For history has too many examples when that trust has been breached.[8]

Yet according to the administration, it can collect all such data as "business records" under Section 215 of the Patriot Act -- without establishing *any* particularized connection between the individuals whose records are sought and a terrorist investigation. And according to the administration, the Fourth Amendment imposes *no limitation* whatsoever on its doing so, because in its view all of us have forfeited our privacy by sharing this information with "third parties" – the businesses that make these services available. The fact that one cannot live in modern America without using these services, the administration contends, is immaterial.

[7] Expert Review Group Report at 110.
[8] Remarks by the President on Review of Signals Intelligence, Jan. 17, 2014, available at http://www.whitehouse.gov/the-press-office/2014/01/17/remarks-president-review-signals-intelligence,

This is a very troubling development for those who believe, as the framers did, that privacy is essential to democracy. As Justice Alito recognized in *United States v. Jones*, which involved the use of much less sophisticated technology -- a GPS -- to monitor the public travel of an automobile for 28 days, our privacy has long rested as much on the practical difficulties of tracking us as on any legal protections:

> In the pre-computer age, the greatest protections of privacy were neither constitutional nor statutory, but practical. Traditional surveillance for any extended period of time was difficult and costly and therefore rarely undertaken. The surveillance at issue in this case--constant monitoring of the location of a vehicle for four weeks--would have required a large team of agents, multiple vehicles, and perhaps aerial assistance. Only an investigation of unusual importance could have justified such an expenditure of law enforcement resources. Devices like the one used in the present case, however, make long-term monitoring relatively easy and cheap.[9]

Just as the GPS makes it cheap to monitor citizens' public travel, so the proliferation of digital information about almost every interaction we have, coupled with advances in computer technology, make it possible to collect and aggregate massive amounts of personally revealing data about all of us. If privacy laws are not adapted to take these developments into account, privacy as we have long known and cherished it will not survive.

The NSA program's defenders invariably claim that the phone records program poses less of a danger to privacy because it collects only the metadata about our phone calls – who we call, who calls us, when we talk, and for how long -- rather than the content of the calls themselves. But former NSA general counsel Stewart Baker has admitted that metadata can be at least as revealing as content itself. He stated:

> Metadata absolutely tells you everything about somebody's life. If you have enough metadata, you don't really need content…. [It's] sort of embarrassing how predictable we are as human beings.[10]

Justice Alito is not the only one to recognize this risk that new technologies pose to our privacy. In the same *Jones* case, Justice Sotomayor wrote that:

> Awareness that the Government may be watching chills associational and expressive freedoms. And the Government's unrestrained power to assemble data that reveal private aspects of identity is susceptible to abuse. The net result is that GPS monitoring--by making available at a relatively low cost such a substantial quantum of intimate information about any person whom the Government, in its

[9] *Jones*, 132 S. Ct. at 963-64 (Alito, J., concurring).
[10] Alan Rusbridger, "The Snowden Leaks and the Public," *The New York Review of Books*, Nov. 21, 2013 (quoting Stewart Baker).

unfettered discretion, chooses to track--may "alter the relationship between citizen and government in a way that is inimical to democratic society."[11]

And more than a decade earlier, in *Kyllo v. United States*,[12] Justice Scalia, writing for the Court majority, similarly recognized the need to adapt the law to preserve traditional expectations of privacy from advances in technology. In that case, the Court ruled that the use of a thermal imaging device to measure heat emanating from the exterior of a house constituted a search. Justice Scalia warned that "[t]o withdraw protection of this minimum expectation would be to permit police technology to erode the privacy guaranteed by the Fourth Amendment."[13] Extending the Fourth Amendment to such practices, he explained, "assures preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted."[14]

In sum, technology has made it possible for the government to know more about us than was even thinkable at the time of the framing. The erosion of practical limits on dragnet surveillance renders legal constraints all the more important. Yet according to the administration's interpretation of existing law, there are few if any legal limits on its ability to collect bulk data on Americans. The Constitution, it has argued, poses no impediment to gathering such information, because under the "third-party disclosure rule" we have all forfeited our expectations of privacy in this information. And there are no substantial statutory limits because, again according to the administration, Section 215 of the USA Patriot Act affirmatively empowers it to gather such data about all of us if it might be useful, at some future point, to search through it for ties to terrorists. The issue goes far beyond telephone data. The same argument would apply to cell phone location data, internet browsing histories, email addressing data, and financial and credit information, and library records. The administration's view of existing law recognizes virtually no limits on the administration's ability to collect and maintain a vast database on everyone.

## II. THE NEED FOR CONGRESSIONAL ACTION

Congress can and should do something about this, by amending the statute that the NSA relies on for its expansive exercise of surveillance power. Congress has repeatedly acted in the past to protect citizens' privacy, while preserving the ability of law enforcement and intelligence agencies to do their jobs responsibly and effectively. It can and should do so again.

As noted above, Justice Alito has expressly noted that Congress is well situated to adjust privacy laws to respond to advances in technology. In fact, Congress has often enacted statutes to protect privacy when the Supreme Court has either not yet addressed the issue, or has ruled that the Constitution's Fourth Amendment itself does not provide protection. Thus, when the

[11] 132 S. Ct. at 956 (Sotomayor, J., concurring) (quoting *United States v. Cuevas-Perez*, 640 F.3d 272, 285 (CA7 2011) (Flaum, J., concurring)).
[12] 533 U.S. 27 (2001).
[13] 533 U.S. at 34.
[14] *Id.*

Supreme Court ruled in *Smith v. Maryland*, 442 U.S. 735 (1979), that "pen registers" did not invade Americans' expectation of privacy, and therefore could be obtained without any Fourth Amendment limitations, Congress enacted statutory restrictions on the use of pen registers. Specifically, 18 U.S.C. § 3122 requires government officials to obtain a court order before installing a pen register, based on a showing that "information likely to be obtained is relevant to an ongoing criminal investigation being conducted by that agency."

Similarly, when the Court ruled in *United States v. Miller*, 425 U.S. 435 (1976), that citizens had no constitutionally protected expectation of privacy in their bank and credit records, meaning that the government could get them without court approval or any showing of necessity or suspicion, Congress enacted the Right to Financial Privacy Act, 12 U.S.C. § 3401 et seq., which provided statutory protections for citizens when the government seeks to obtain their bank and credit card records.

Congress has protected the privacy of video rental records, requiring a warrant, subpoena, or court order for the disclosure, even though the Court's "third-party disclosure" rule would likely deny constitutional protection to such records. 18 U.S.C. § 2710.

When the Supreme Court in *Zurcher v. Stanford Daily*, 436 U.S. 547 (1978), declined to interpret the Fourth Amendment to impose any special restriction on the government's ability to search innocent third parties or the press for evidence of crime, Congress enacted the Privacy Protection Act of 1980, 42 U.S.C. § 2000aa, which afforded both innocent third parties and the press protections as a statutory matter that the Supreme Court had refused to provide as a constitutional matter.

The Foreign Intelligence Surveillance Act, 50 U.S.C. § 1801 et seq., regulates the government's ability to conduct wiretaps and searches for foreign intelligence gathering purposes, despite the fact that the Supreme Court left open whether foreign intelligence gathering is subject to Fourth Amendment restrictions.[15]

Section 215 of the USA Patriot Act itself imposes statutory restrictions on access to business records that might otherwise fall under the "third-party disclosure" rule, and therefore might not be subject to Fourth Amendment limitations.

And Section 702 of the FISA Amendments Act of 2008, 50 U.S.C. § 1881a, imposes statutory restrictions on surveillance directed at foreign nationals living abroad, even though the Supreme Court has ruled that at least in some circumstances, the Fourth Amendment does not limit the government's ability to search foreign nationals outside the United States.[16]

Thus, Congress has a long record of affording more protection to Americans' privacy than the Supreme Court has interpreted the Fourth Amendment to provide. In some scenarios,

[15] *United States v. United States District Court*, 407 U.S. 297, 308 (1972).
[16] *United States v. Verdugo-Urquidez*, 494 U.S. 259 (1990).

Congress acted in response to Supreme Court decisions that at least arguably were insufficiently attentive to privacy demands. In other settings, Congress acted to fill a gap where the Supreme Court had failed to clarify the extent of Fourth Amendment protection, if any. In any event, this history demonstrates that Congress plays an essential role in safeguarding the privacy of Americans, and that it plays a role that is distinct from that played by the Court.

There is a particular need for congressional action here, because the executive and the FISC have interpreted an existing statute, Section 215, in ways that few if any members of Congress would have supported. That statute authorizes the government to obtain a court order for the production of business records only where they are "relevant to an authorized [foreign intelligence] investigation." As the Privacy and Civil Liberties Oversight Board has convincingly and exhaustively demonstrated, Section 215's requirement that only records "relevant to an authorized investigation" does not support the collection of all telephone metadata on every American, as the NSA has been collecting.[17]

The government has argued – and the FISC has accepted[18] -- that collecting all Americans' phone records and maintaining them for five years is "relevant" to a terrorism investigation because at some future time the government might want to search those records for links to terror suspects. In other words, all of our phone numbers are "relevant" not because any of us has any connection to terrorism, but because the NSA might someday find it useful to search through them all for as yet unspecified links to terrorism.

On this theory, the Privacy Board noted, "virtually all information may be relevant to counterterrorism and therefore subject to collection by the government." (60) Indeed, "while terrorists use telephone communications to facilitate their plans they also write emails, open bank accounts, use debit and credit cards, send money orders, rent vehicles book hotel rooms, sign leases, borrow library books, and visit websites."[19] On the administration's view of Section 215, it could collect records on all American's email, internet, banking, credit, and library activities, because at some point those records might be useful to a terrorism search. There is no limiting principle. Yet surely Congress intended to impose a limit of relevance when it authorized not the collection of all business records of all Americans, but only of records "relevant to an authorized investigation." Yet the administration's interpretation renders meaningless the restriction of obtainable documents to "relevant" records. As the Privacy Board put it, this interpretation

[17] Privacy Board Report, at 57-102.

[18] NSA defenders often claim that 15 federal judges of the FISC court have ruled that the Section 215 program is legally authorized. In a very technical sense, that may be true. But it is misleading, because all but one FISC judge never actually wrote an opinion assessing the legality of the program. Instead, as noted in the Introduction, the FISC approved of the telephone records program in May 2006 without offering any explanation for its rationale, and until August 2013, none of the many judges who routinely approved of the program's extension at 90-day intervals offered any explanation for their rationale. The only FISC judge who has actually set forth a rationale for finding the program legal is Judge Claire Eagan, on August 29, 2013, two months after the program was revealed to the public. Amended Memorandum Opinion, *In re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things*, No. BR 13-109 (FISA Ct. Agu. 29, 2013).

[19] Privacy Board Report at 62.

"supplies a license for nearly unlimited government al acquisition of other kinds of transactional information."[20]

In addition, as the Privacy Board has demonstrated, the government's novel construction of "relevant" finds no support in any of the analogous situations in which the government or private parties are authorized to obtain "relevant" documents. The government has cited to no grand jury subpoena or civil discovery order in the history of American litigation that has authorized the collection of records on every American.[21]

The administration's interpretation of Section 215 also conflicts with other statutes that impose more stringent restrictions on collection of the very same data that the NSA has been gathering under Section 215. For example, another section of FISA, 50 U.S.C. §1842, authorizes the use of "pen registers" and "trap and trace" devices to collect the same phone data that the NSA is now gathering under Section 215. Yet §1842 restricts the use of pen registers and trap and trace devices to specified phone numbers.[22] The administration's interpretation of Section 215 effectively allows it to evade the requirements of the pen register provision and get the same information on every American without specifying anyone's numbers as a target.

The administration's reading of Section 215 also conflicts with the Electronic Communications Privacy Act (ECPA), 18 U.S.C. § 2510 et seq., which expressly addresses phone and other electronic communication records and states that a provider "shall not knowingly divulge a record or other information pertaining to a subscriber to or to a customer of such service … to any governmental entity" except pursuant to specifically enumerated circumstances.[23] The enumerated circumstances do *not* include a court order under Section 215 (but do include a court order under ECPA).

Thus, the administration's interpretation of Section 215 is at odds with the plain language of the statute, with all precedent interpreting the term "relevant" in analogous settings, and with other parts of FISA and ECPA. Yet in defense of its counterintuitive interpretation, the administration has cited to no evidence that at the time Congress amended Section 215 even a single member of Congress thought that the stature was giving the NSA authority to collect business records on every American. To the contrary, Representative Sensenbrenner, one of the Patriot Act's architects in the House, has stated that he never intended to authorize such dragnet collection when authorizing the FBI to obtain business records "relevant to an authorized investigation."[24]

---

[20] *Id*.
[21] *Id*. at 63-81 (reviewing interpretation and application of "relevance" in civil discovery, grand jury subpoenas, and administrative subpoenas).
[22] *See* 50 U.S.C. § 1842(d)2)(A)(iii).
[23] 18 U.S.C. §§ 2702(c), 2703(c).
[24] *See, e.g.*, Letter of Sensenbrenner to Attorney General Eric Holder, Sept. 6, 2013, available at http://sensenbrenner.house.gov/uploadedfiles/sensenbrenner_letter_to_attorney_general_eric_holder.pdf.

Congress should act now in order to make clear that it did not intend to give the government access to all Americans' phone records, and more fundamentally, to ensure that Americans do not forfeit their privacy by default simply through advances in technology and secret interpretations of law.

## III. THE USA FREEDOM ACT

The USA Freedom Act would end the NSA's bulk collection of phone records, and ensure that the government cannot secretly collect other records of Americans' private activities in bulk. It would amend Section 215 to authorize collection of business records only where the government could show that they pertain to a foreign agent or foreign power, the activities of a suspected agent of a foreign power, or an individual in contact with or known to a suspected agent of a foreign power. Thus, it would allow the government to seek business records in order to confirm or deny potential connections between suspected terrorists and foreign agents, on the one hand, and Americans on the other. But it would require the government to do so through targeted inquiries, not dragnet collections and searches that amass records on the private activities of every American.

The USA Freedom Act would sensibly impose the same restriction on National Security Letters and pen registers and trap and trace orders, to ensure that these authorities do not become end runs around the limits on Section 215. As the President's Review Group noted, National Security Letters allow the FBI to obtain without any court review some of the same business records that, under Section 215, require a court order. Of even greater concern, however, is that the NSL statute uses the same "relevance" standard used in Section 215. If the administration reads that standard to permit unlimited collection of business records under Section 215, the NSL authority could also be used just as broadly. Accordingly, the USA Freedom Act would amend these statutes by adding the same nexus requirement that it would add to Section 215.

These amendments, which are consistent with the Privacy Board's recommendation to terminate bulk collection, are preferable to the approach taken by President Obama in his NSA speech. There, he proposed that Americans' phone records would continue to be collected in bulk, but held by some private entity, to be identified later. Leaving the data in the hands of a private entity, however, does not solve the problem presented by dragnet collection of private information. Under the President's proposal, dragnet collection would continue. The focus of reform should be on ending dragnet collection altogether, and requiring law enforcement and intelligence agencies to use the targeted approach that the Constitution requires, and that maintains respect for Americans' privacy while at the same time affording government the tools to keep us safe. That is the approach the USA Freedom Act takes.

The USA Freedom Act also contains several measures that would increase transparency and accountability with respect to foreign intelligence gathering. These are critically important

reforms. As the revelations of the last several months have made clear, when intelligence agencies and the FISC operate entirely in secret, they are prone to adopting expansive measures that would likely be unacceptable if subjected to public scrutiny. There is of course a legitimate place for secrecy with respect to intelligence gathering. The American public does not need to know the details of every wiretap or order authorizing the collection of specific business records. But when the government adopts surveillance practices that affect literally every one of its citizens, and does so entirely in secret, secrecy has gone too far. As long as the telephone metadata program was secret, neither the executive, the courts, nor Congress did anything to stop it. Now that it has been revealed to the public, the President has proposed reforms, one court has declared the program likely unconstitutional, and Congress is considering numerous bills to rein in the NSA. That course of events illustrates the problem with secrecy. The institutional checks and balances established by the Constitution are important safeguards of liberty, but as this episode has revealed, they are insufficient without the light of public scrutiny.

In order to focus on the Section 215 program, I have not addressed other reforms in the USA Freedom Act, including new limitations on Section 702 of the FISA Amendments Act, and reforms to the FISC. I support those reforms as well, but will leave to others more extended discussion of them.

## CONCLUSION

Three principles should guide Congress as it confronts the challenge of regulating foreign intelligence surveillance. First, we should not let advances in technology deprive us of our privacy by default. We can enjoy the tremendous advantages and conveniences of the digital age and still preserve our privacy. But in order to do so, Congress must enact rules to limit the power of new technologies to impose dragnet surveillance on all of us through the bulk collection of data revealing personal information. Second, Congress is especially well suited to enact the rules necessary to preserve privacy in the digital age, as it can consider the issues in a more wide-ranging way than the courts, and historically has had a better sense of the privacy that Americans expect. And third, the principle that has long been used to balance privacy and security – that the government's security interests permit intrusions on privacy when the government develops individualized suspicion – remains the appropriate guidepost as we go forward. The very fact that the government has so little to show in terms of security benefits from seven years of collecting every American's phone records underscores that this sort of dragnet approach is not necessary to our security.

Privacy remains just as essential today as it was when the Fourth Amendment was adopted. But the challenges to maintaining privacy are much more substantial, because technology has given the government the tools to invade our privacy in ways that were inconceivable a generation ago. If we are to preserve the privacy that remains critical to a healthy democracy, Congress must act.