

Oversight Hearing on FISA Surveillance Programs

Committee on the Judiciary

United States Senate

July 31, 2013

Statement of Stewart A. Baker

Partner, Steptoe & Johnson LLP

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

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. LAW REPORT 2, May 1997, at 1-2.

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.

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

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).

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 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.

Section 215 and the Collection-First Model

That provides a useful frame for the most surprising disclosure made by Edward Snowden – that NSA collects telephone metadata (*e.g.*, the called number, calling number, duration of call, etc., but not the call content) for all calls into, out of, or within the United States. Out of context – and Snowden worked hard to make sure it *was* taken out of context – this is a troubling disclosure. How can all of that data possibly be “relevant to an authorized investigation” as the law requires?

But context is everything here. It turns out that collecting the data isn't the same as actually looking at it. Robert Litt, General Counsel of the Director for National Intelligence, has made clear that there are court-ordered rules designed to make sure that government officials only look at relevant records: “The metadata that is acquired and kept under this program can only be queried when there is reasonable suspicion, based on specific, articulable facts, that a particular telephone number is associated with specified foreign terrorist organizations. And the only purpose for which we can make that query is to identify contacts.”⁵ And in fact these rules have been interpreted so strictly that last year the agency only actually looked at records for 300 subscribers.⁶

Still, isn't the government “seizing” millions of records without a warrant or probable cause, even if it's not searching them? “How can that be constitutional?” you might ask.

⁵ Robert Litt, General Counsel, Office of the Director of National Intelligence, Newseum Special Program - NSA Surveillance Leaks: Facts and Fiction (June 26, 2013) (transcript available at <http://www.dni.gov/index.php/newsroom/speeches-and-interviews/195-speeches-interviews-2013/887-transcript-newseum-special-program-nsa-surveillance-leaks-facts-and-fiction>).

⁶ *Id.*

Very easily, as it happens. The Supreme Court has held that such records are not protected by the Fourth Amendment, since they've already been given to a third party.⁷

And even if the Fourth Amendment applied, at bottom it requires only that seizures be reasonable. The Court has recognized more than half a dozen instances where searches and seizures are reasonable even in the absence of probable cause and a warrant.⁸ They range from drug screening to border searches. There can hardly be doubt that the need to protect national security fits within this doctrine as well, particularly when waiting to conduct a traditional search won't work. Call data doesn't last. If the government doesn't preserve the data now, the government may not be able to search it later, when the need arises.

In short, there's less difference between this "collection first" program and the usual law enforcement data search than first meets the eye. In the standard law enforcement search, the government establishes the relevance of its inquiry and is then allowed to collect and search the data. In the new collection-first model, the government collects the data and then must establish the relevance of each inquiry before it's allowed to conduct a search.

I know it's fashionable to say, "But what if I don't trust the government to follow the rules? Isn't it dangerous to let it collect all that data?" The answer is that the risk of rule-breaking is pretty much the same whether the collection comes first or second. Either way, you have to count on the government to tell the truth to the court, and you have to count on the court to apply the rules. If you don't trust them to do that, then neither model offers much protection against abuses.

But if in fact abuses were common, we'd know it by now. Today, law enforcement agencies collect several hundred thousand telephone billing records a year using nothing

⁷ *Smith v. Maryland*, 442 U.S. 735, 743-44 (1979) (affirming the Court's previous holdings that "the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed") (citing *U.S. v. Miller*, 425 U.S. 435, 442 (1976)).

⁸ See, e.g., *O'Connor v. Ortega*, 480 U.S. 709, 720 (1987) (plurality opinion) (concluding that, in limited circumstances, a search unsupported by either warrant or probable cause can be constitutional when "special needs" other than the normal need for law enforcement provide sufficient justification); *Griffin v. Wisconsin*, 483 U.S. 868, 873 (1987) (holding Wisconsin Supreme Court's interpretation of regulation requiring "reasonable grounds" for warrantless search of probationer's residence satisfies the Fourth Amendment reasonableness requirement); *Vernonia School Dist. 47J v. Acton*, 515 U.S. 646, 652-653 (1995); *Wyoming v. Houghton*, 526 U.S. 295, 300 (1999) (asserting that when historical analysis of common law at the time of the Fourth Amendment proves inconclusive as to what protections were envisioned, the Court must "evaluate the search or seizure under traditional standards of reasonableness by assessing, on the one hand, the degree to which it intrudes upon an individual's privacy and, on the other, the degree to which it is needed for the promotion of legitimate governmental interests"); *Packwood v. Senate Select Committee on Ethics*, 510 U.S. 1319, 1321 (1994) (observing the uncontested application of a Fourth Amendment legal standard that "balanced applicant's privacy interests against the importance of the governmental interests. The court concluded that the latter outweighed the former"); *U.S. v. Cantley*, 130 F.3d 1371, 1375 (10th Cir., 1997) (noting that the Supreme Court "has recognized exceptions to the warrant requirement for certain "special needs" of law enforcement, including a state's parole system").

but a subpoena.⁹ That means you're roughly a thousand times more likely to have your telephone calling patterns reviewed by a law enforcement agency than by NSA. (And the chance that law enforcement will look at your records is itself low, around 0.25% in the case of one carrier¹⁰). So it appears that law enforcement has been gaining access to our call metadata for as long as billing records have existed – nearly a century. If this were the road to Orwell's 1984, surely we'd be there by now, and without any help from NSA's 300 searches.

Section 702 and “PRISM”

This brings us to PRISM and the second of the Snowden stories to be released. Without the surprise of the phone metadata order, the PRISM slide show released by Snowden would have been much less newsworthy. Indeed, the parts of the PRISM story that were true aren't actually new and the parts that were new aren't actually true.

Let's start with what's true. Despite the noise around PRISM, the slides tell us very little that the law itself doesn't tell us. Section 702 says that the government may target non-U.S. persons “reasonably believed to be located outside the United States to acquire foreign intelligence information.” It covers activities with a connection to the United States and is therefore subject to greater oversight than foreign intelligence gathered outside the United States. Although the Attorney General and the Director of National Intelligence can authorize collection annually, the collection and use of the data is covered by strict targeting and minimization procedures that are subject to judicial review and aimed at protecting U.S. persons as well as other persons located inside the United States.

That's what the law itself says, and the Snowden slides simply add voyeuristic details about the collection. Everyone already knew that the government had the power to do this because, unlike many countries, we codify these things in law. It should come as no surprise then that the government has been using its power to protect all of us.

There was one surprise in those stories though. That's the part that was new but not true. When the story originally broke, reporters at the *Guardian* and the *Washington Post* made it look as if the NSA had direct, unfettered access to private service providers' networks and that they were downloading materials at will. To be fair, the slides were

⁹ In 2012, Rep. Markey sent letters to a large number of cell phone companies, asking among other things how many law enforcement requests for subscriber records the companies received over the past five years. The three largest carriers alone reported receiving more than a million law enforcement subpoenas a year. *Letters to mobile carriers regarding use of cell phone tracking by law enforcement*, CONGRESSMAN ED MARKEY, <http://markey.house.gov/content/letters-mobile-carriers-reagrding-use-cell-phone-tracking-law-enforcement> (last visited July 15, 2013).

¹⁰ Letter from Timothy P. McKone, Exec. Vice President, AT&T, to Congressman Ed Markey 3 (May 29, 2012), <http://markey.house.gov/sites/markey.house.gov/files/documents/AT%26T%20Response%20to%20Rep.%20Markey.pdf>.

confusing on this point, talking about getting data “directly from the servers” of private companies. But that phrase is at best ambiguous; it could easily mean that NSA serves a lawful order on the companies and the companies search for and provide the data from their servers. In fact, everyone with knowledge, from the DNI to the companies in question, has confirmed that interpretation while denying that NSA has unfettered access to directly search the private servers. In short, it now looks as though the *Washington Post* and the *Guardian* hyped this aspect of their story to spur a public debate about NSA surveillance.

In short, in both section 215 and section 702, the government has found a reasonable way to square intelligence-gathering necessities with changing technology. Now that they’ve been exposed to the light of day, these programs are not at all hard to justify. But we cannot go on exposing every collection technique to the light of day just to satisfy everyone that the programs are appropriate. The exposure itself will diminish their effectiveness. Even a fair debate in the open will cause great harm.

And this was never meant to be a fair debate. Snowden and his allies in the press had copies of the minimization and targeting guidelines; they surely knew that the guidelines made the programs look far more responsible. So they suppressed them, waiting a full two weeks – while the controversy grew and took the shape they preferred – before releasing the documents. Since no self-respecting reporter withholds relevant information from the public, it’s only fair to conclude that this was an act of advocacy, not journalism. Perhaps the reporters lost their bearings; perhaps the timing was controlled by advocates. Either way, the public was manipulated, not informed.

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? I think the current debate exposes two serious difficulties in using law to regulate intelligence gathering.

1. 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.¹¹ 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

¹¹ 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.

not just improve privacy enforcement, it likely would have flagged both Bradley Manning and Edward Snowden for their unusual network browsing habits.

2. The Rest of the World Has a Ringside Seat – And It Wants a Vote, Too

There's a second reason why the American experiment in creating a detailed set of legal restraints on intelligence gathering is facing unexpected difficulties. The purpose of those restraints is to protect Americans from the intelligence collection techniques we use on foreign governments and nationals. At every turn, the laws and regulations reassure Americans that they will not be targeted by their own intelligence services. This makes plenty of sense from a policy and civil liberties point of view. Intelligence gathering isn't pretty, and it isn't patty cake. On occasion, the survival of the country may depend on good intelligence. Wars are won and lives are lost when intelligence succeeds or fails. Nations do whatever they can to collect information that might affect their future so dramatically. After a long era of national naïveté, when we thought that gentlemen didn't read other gentlemen's mail and when intercepting even diplomatic radio signals was illegal, the United States found itself thrust by World War II and the Cold War into the intelligence business, and now we play by the same rules as the rest of the world.

The purpose of much intelligence law and regulation is to make sure we do not apply those rules to our own citizens. On the whole, I'm confident that we have gone about as far in pursuit of that goal as we can without seriously compromising our ability to conduct foreign intelligence. And we've spelled those assurances out in unprecedented detail. All of that should – and largely has – left the majority of Americans satisfied that intelligence under law is working reasonably well.

The problem is that Americans aren't the only people who read our laws or follow our debates. So does the rest of the world. And it doesn't take much comfort from legal assurances that the privacy interests of *Americans* are well protected from our intelligence agencies' reach. So, while the debate over U.S. intelligence gathering is already beginning to recede in this country, the storm is still gathering abroad. Many other countries have complained about the idea that NSA may be spying on their citizens. Politicians in France, Brazil, Germany, the Netherlands, the United Kingdom, Belgium, and Romania, among others, have expressed shock and called for investigations into PRISM. On July 4, the European Parliament passed a resolution calling for a range of possible actions, such as delaying trade talks and suspending law enforcement and intelligence agreements with the United States over allegations that the United States gathered intelligence on European diplomats.¹²

¹² European Parliament resolution of 4 July 2013 on the US National Security Agency surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' privacy (2013/2682(RSP)) at <http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P7-TA-2013-0322&language=EN> [hereinafter *European Parliament Resolution*].

Some of this is just hypocrisy. Shortly after President Hollande demanded that the U.S. “immediately stop” its intercepts¹³ and the French Interior Minister used his position as guest of honor at a July 4th celebration to chide the United States for its intercepts, *Le Monde* disclosed what both French officials well knew – that France has its own program for large-scale interception of international telecommunications traffic.¹⁴

But some of reaction is grounded in ignorance. Thanks to our open debates and detailed legislative limits on intelligence gathering, Europeans know far more about U.S. intelligence programs than about their own. The same is true around the world.

As a result, it’s easy for European politicians to persuade their publics that the United States is uniquely intrusive in the way it conducts law enforcement and intelligence gathering from electronic communications providers. In fact, the reverse is true.

Practically every comparative study of law enforcement and security practice shows that the United States imposes more restriction on its agencies and protects its citizens’ privacy rights from government surveillance more carefully than Europe.

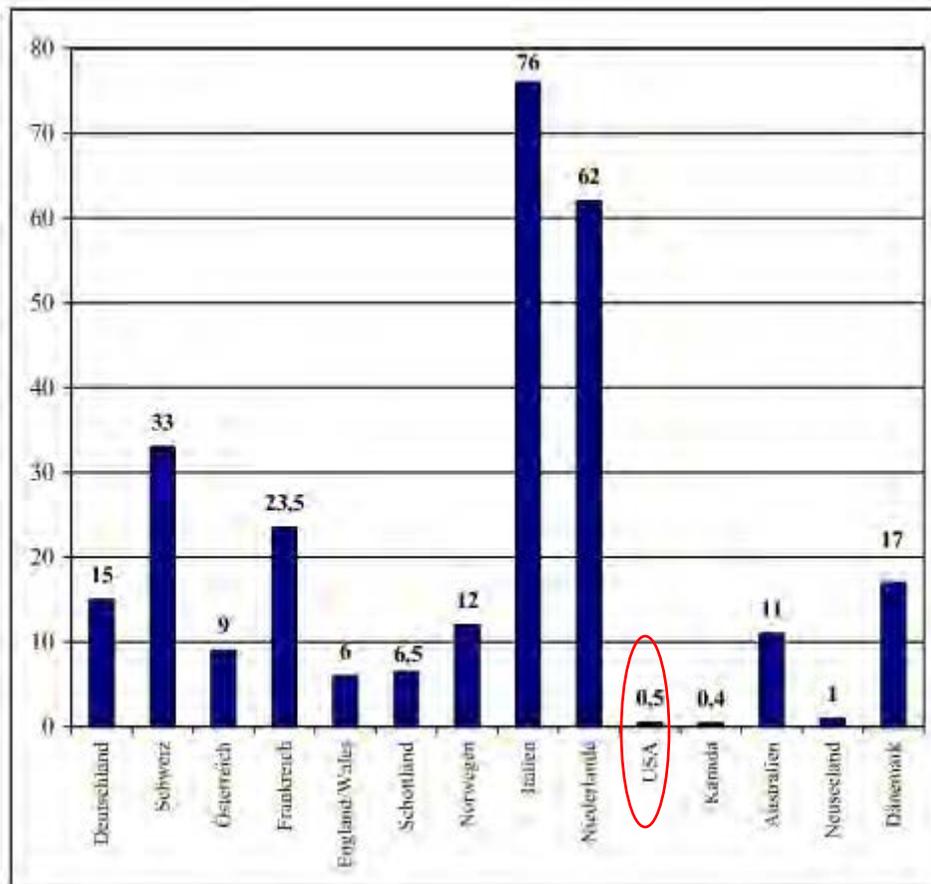
I’ve included below two figures that illustrate this phenomenon. One is from a study done by the Max Planck Institute, estimating the number of surveillance orders per 100,000 people in several countries. While the statistics in each are not exactly comparable, the chart published in that study shows an unmistakable overall trend. The number of U.S. orders is circled, because it’s practically invisible next to most European nations; indeed, an Italian or Dutch citizen is more than a hundred times more likely to be wiretapped by his government than an American.¹⁵

¹³ Sébastien Seibt, *France’s ‘hypocritical’ spying claims ‘hide real scandal’*, FRANCE24 (July 3, 2013), <http://www.france24.com/en/20130702-france-usa-spying-snowden-hollande-nsa-prism-hypocritical>.

¹⁴ Jacques Follorou and Franck Johannès, *In English: Revelations on the French Big Brother*, LE MONDE (July 4, 2013, 5:24 PM), http://www.lemonde.fr/societe/article/2013/07/04/revelations-on-the-french-big-brother_3442665_3224.html.

¹⁵ Hans-Jörg Albrecht, et al., *Legal Reality and Efficiency of the Surveillance of Telecommunications*, MAX PLANCK INSTITUTE 104 (2003), http://www.gesmat.bundesgerichtshof.de/gesetzesmaterialien/16_wp/telekueberw/rechtswirklichkeit_%20abschlussbericht.pdf.

Which countries do the most surveillance per capita?



Similarly, the PRISM program is widely believed to show a uniquely American enthusiasm for collecting data from service providers. In fact, it owes that reputation in part to detailed statutory provisions that are meant to protect privacy but that also spell out how the program works.

European regimes, by and large, offer far less protection against arbitrary collection of personal data – and expose their programs to far less public scrutiny. One recent study showed that, out of a dozen advanced democracies, only two – the United States and Japan – impose serious limits on what electronic data private companies can give to the government without legal process. In most other countries, and particularly in Europe,

little or no process is required before a provider hands over information about subscribers.¹⁶

Which countries allow providers simply to volunteer information to government investigators instead of requiring lawful process?

	Can the government use legal orders to force cloud providers to disclose customer information – as in PRISM?	Can the government skip the legal orders and just get the cloud provider to disclose customer information voluntarily?
Australia	Yes	Yes
Canada	Yes	Yes*
Denmark	Yes	Yes*
France	Yes	Yes**
Germany	Yes	Yes**
Ireland	Yes	Yes*
Japan	Yes	No
Spain	Yes	Yes*
UK	Yes	Yes*
USA	Yes	No

*Voluntary disclosure of personal data requires valid reason

**Some restrictions on voluntary disclosure of personal data without a valid reason and of some telecommunications data

¹⁶ Winston Maxwell & Christopher Wolf, *A Global Reality: Governmental Access to Data in the Cloud*, HOGAN LOVELLS (July 18, 2012).

At most, European providers must have a good reason for sharing personal data, but assisting law enforcement investigations is highly likely to satisfy this requirement. In the United States, such sharing is prohibited in the absence of legal process.

Despite the evidence, however, it is an article of faith in Europe that the United States lags Europe in respect for citizens' rights when collecting data for security and law enforcement purposes. Again, this is the unfortunate result of our commitment to regulating our intelligence services in a more open fashion than other countries.

The U. S. government has learned to live with Europe's misplaced zeal for moral tutelage where data collection is concerned. Our government can ride out this storm as it has ridden out others. But the antagonism spawned by Snowden's disclosures could have more serious consequences for our information technology companies.

Many countries around the world have launched investigations designed to punish American companies for complying with American law. Some of the politicians and data protection agencies pressing for sanctions are simply ignorant of their own nation's aggressive use of surveillance, others are jumping at any opportunity to harm U.S. security interests. But the fact remains that the price of obeying U.S. law could be very high for our information technology sector.

Foreign officials are seizing on the disclosures to fuel a new kind of information protectionism. During a French parliament hearing, France's Minister for the Digital Economy declared that, if the report about PRISM "turns out to be true, it makes [it] relatively relevant to locate datacenters and servers in [French] national territory in order to better ensure data security."¹⁷ Germany's Interior Minister was even more explicit, saying, "Whoever fears their communication is being intercepted in any way should use services that don't go through American servers."¹⁸ And Neelie Kroes, Vice President of the European Commission, said, "If European cloud customers cannot trust the United States government or their assurances, then maybe they won't trust US cloud providers either. That is my guess. And if I am right then there are multi-billion euro consequences for American companies."¹⁹

Hurting U.S. information technology firms this way is a kind of three-fer for European officials. It boosts the local IT industry, it assures more data for Europe's own surveillance systems, and it hurts U.S. intelligence.

¹⁷ Valéry Marchive *France hopes to turn PRISM worries into cloud opportunities*, ZDNET (June 21, 2013, 9:02 GMT), <http://www.zdnet.com/france-hopes-to-turn-prism-worries-into-cloud-opportunities-7000017089/>.

¹⁸ *German minister: Drop US sites if you fear spying*, ASSOCIATED PRESS (July 3, 2013), http://m.apnews.com/ap/db_307122/contentdetail.htm?contentguid=OmnMPwXK.

¹⁹ Neelie Kroes, Vice President, European Commission, Statement after the meeting of European Cloud Partnership Board, Tallinn, Estonia (July 4, 2013) (transcript available at http://europa.eu/rapid/press-release_MEMO-13-654_en.htm).

The European Parliament has been particularly aggressive in condemning the program as a violation of European human rights.²⁰ Its resolution pulls out all the stops, threatening sanctions if the United States does not modify its intelligence programs to provide privacy protections for European nationals. The resolution raises the prospect of suspending two anti-terror agreements with the United States on passenger and financial data, it “demands” U.S. security clearances for European officials so they can review all the documents about PRISM, and it threatens US-EU trade talks as well as the Safe Harbor that allows companies to move data freely across the Atlantic.

This may be the most egregious double standard to come out of Europe yet. Unlike our section 215 program, the EU doesn’t have a big metadata database. But that’s because Europe doesn’t need one. Instead, the European Parliament passed a measure forcing all of its information technology providers to create their own metadata databases so that law enforcement and security agencies could conveniently search up to two years’ worth of logs. These databases are full of data about American citizens, and under EU law any database held anywhere in Europe is open to search (and quite likely to “voluntary” disclosure) at the request of any government agency anywhere between Bulgaria and Portugal.

I have seen this movie before, too. During my tenure at Homeland Security, European officials tried to keep the United States from easily accessing travel reservation data to screen for terrorists hoping to blow up planes bound for the United States. In order to bring the United States to the table, European officials threatened to impose sanctions not on the government but on air carriers who cooperated with the data program.²¹ Similarly, to limit U.S. access to terror finance information, European data protection authorities threatened the interbank transfer company, SWIFT, with criminal prosecution and fines for giving the U.S. access to transfer data.²² In the end, the threat of sanctions forced SWIFT to keep a large volume of its data in Europe and to deny U.S. authorities access to it.

Now, whenever Europe has a beef with U.S. use of data in counterterrorism programs, it threatens not the U.S. government but U.S. companies. The European Parliament is simply returning to that same playbook. There is every reason to believe that European governments, and probably some imitators in Latin America and elsewhere, will hold U.S. information technology companies hostage in order to show their unhappiness at the PRISM disclosures.

3. What Congress Should Do About It

As a result, 2013 is going to be a bad year for companies that complied with U.S. law. We need to recognize that our government put them in this position. Not just the

²⁰ *European Parliament Resolution, supra* note 12.

²¹ *BAKER, supra* note 3, at 114-15.

²² *Id.* at 145-51.

executive branch that served those orders, but Congress too, which has debated and written intelligence laws as though the rest of the world wasn't listening.

The U.S. government, all of it, has left U.S. companies seriously at risk for doing nothing more than their duty under U.S. law. And the U.S. government, all of it, has a responsibility to protect U.S. companies from the resulting foreign government attacks.

The executive branch has a responsibility to interpose itself between the companies and foreign governments. The flap over Snowden's disclosures is a dispute between governments, and it must be kept in those channels. Diplomatic, intelligence, and law enforcement partners in every other country should hear the same message: "If you want to talk about U.S. intelligence programs, you can talk to us – but not to U.S. companies and individuals; they are prohibited by law from discussing those programs."

Congress too needs to speak up on this question. European politicians feel free to demand security clearances and a vote on U.S. data programs in part because they think Congress and the American public share their views. It's time to make clear to other countries that we do not welcome foreign regulation of U.S. security arrangements.

There are many ways to convey that message. Congress could – should – adopt its own resolution rejecting the European Parliament's.

Congress could prohibit U.S. agencies from providing intelligence and law enforcement assistance or information to nations that have harassed or threatened U.S. companies for assisting their government – unless the agency head decides that providing a particular piece of information will also protect U.S. security.

It could require similar review procedures to make sure that Mutual Legal Assistance Treaties do not provide assistance to nations that try to punish U.S. companies for obeying U.S. law.

And it could match the European Parliament's willingness to reopen the travel data and terror finance pacts with its own, prescribing in law that if the agreements are reopened they must be amended to include an anti-hypocrisy clause ("no privacy obligations may be imposed on U.S. agencies that have not already been imposed on European agencies") as well as an anti-hostage-taking clause ("concerns about government conduct will be raised between governments and not by threatening private actors with inconsistent legal obligations").

And, just to show that this particular road runs in both directions, perhaps Congress could mandate an investigation into how much data about individual Americans is being retained by European companies, how often it is accessed by European governments, and whether access meets our constitutional and legal standards.

Conclusion

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.

Senate Judiciary Committee Hearing
“Strengthening Privacy Rights and National Security:
Oversight of FISA Surveillance Programs”
July 31, 2013

Prepared Remarks of James G. Carr,
Sr. U.S. District Judge
N.D. Ohio

Having been asked to appear here following the publication in the *New York Times* on July 23, 2013, of an op-ed article suggesting an amendment to the Foreign Intelligence Act, I do so with the caveat that whatever I say – or have written – on the subject of the op-ed expresses my views alone. I do not mean to bypass the normal process by which the Judiciary proposes legislation. I speak for myself and no one else.

The proposal I made in the op-ed piece is whether it would be worthwhile for the judges of the Foreign Intelligence Surveillance, when a government FISA application raises a new or novel issue of constitutional or statutory interpretation, to have discretion to designate a previously security-cleared attorney to challenge the government’s request.

Such appointment would not be frequent, and would not occur in the routine kind of cases making up the day in, day out docket of the Foreign Intelligence Surveillance Court (FISC). Rarely does a FISA application present any challenging issues under the statute. The probable cause standard is much lower than for a conventional search warrant. Once the government meets that standard, judges must issue the FISA order.

Once in a very great while, however, a FISA application raises a novel, substantial, and very difficult issue of law. In such circumstances, the FISC judge (or judges, sitting en banc) may desire to hear not just the government’s views in support of the request, but reasons from an independent attorney as to why the court should not issue the order in whole or part.

This process would give the court the benefit of the give and take that is the hallmark of the adversarial process.

In addition, review by the Foreign Intelligence Court of Review would occur, as it does not now, where the government had prevailed before the FISC. Today, only the government, as the only party before the FISC, is in a position to appeal, which it is not likely to do where the FISC has granted its request.

Where such review were available and pursued, public concern about the decisions of the FISC should moderate. This would be so, whether or not the opinion of the Court of Review became public.

If implemented, my recommendation about appointment of counsel would also make possible ultimate review by the Supreme Court.

I can foresee at least one objection to what I propose. Namely, no one besides the government appears when the government seeks an ordinary search warrant in a conventional criminal investigation. But the subject of a conventional Fourth Amendment search warrant knows of its execution, can challenge its lawfulness if indicted, and can, even if not indicted, seek to recover seized property or possibly sue for damages.

In contrast, except in very, very rare instances, suppression or other means of challenging the lawfulness of a FISA order is simply not available to the subject of a FISA order. Even on the infrequent occasion when a FISA target becomes charged in a criminal case, he will, as a result of the procedures mandated in the Classified Information Procedures Act almost never have the opportunity to challenge the FISA order.

Thus, although all conventional search warrants issue *ex parte*, their execution informs the subject of the warrant's issuance. Once the subject knows of the warrant, the law gives that subject several ways in which to challenge the lawfulness of the warrant and search. This is not so with a FISA order.

Another concern would arise where the FISC must, due to emergency circumstances, act immediately. The FISA already authorizes the government to act without a FISA order in emergency circumstances. In such cases, it must still seek *post hoc* FISC approval for the surveillance. In such circumstances, the FISC judge could designate counsel at that stage. In any event, new constitutional issues probably would not arise in emergency circumstances.

My recommendation, while offering some substantial potential benefits to the court's processes and public generally, is very modest. It would not affect the court's day to day operations. It would remain for an individual judge to determine whether to invoke this option on the infrequent occasion that the judge concluded doing so would be useful.

Finally, I emphasize again that these comments, and anything that I may say in response to the Committee's questions, express my views alone, not those of the Federal Judiciary, any other judge, or any one else. While I think what I ask the Committee to consider is worthwhile, only time can tell whether others do as well.

Thank you for this opportunity to submit these Remarks and the attached copy of the op-ed piece which is the occasion for my being here.

###

Opening Statement of Deputy Attorney General James M. Cole
Before the Senate Judiciary Committee, July 31, 2013, 9:00am

Thank you, Mr. Chairman, Mr. Ranking Member and members of the committee, for inviting us here to speak about the 215 business records program and section 702 of FISA. With these programs and other intelligence activities, we are constantly seeking to achieve the right balance between the protection of national security and the protection of privacy and civil liberties. We believe these two programs have achieved the right balance.

First of all, both programs are conducted under public statutes passed and later reauthorized by Congress. Neither is a program that has been hidden away or off the books. In fact, all three branches of government play a significant role in the oversight of these programs. The Judiciary – through the Foreign Intelligence Surveillance Court – plays a role in authorizing the programs and overseeing compliance; the Executive Branch conducts extensive internal reviews to ensure compliance; and Congress passes the laws, oversees our implementation of those laws, and determines whether or not the current laws should be reauthorized and in what form.

Let me explain how this has worked in the context of the 215 program. The 215 program involves the collection of metadata from telephone calls. These are

telephone records maintained by the phone companies. They include the number a call was dialed from, the number the call was dialed to, the date and time of the call, and the length of the call. The records do not include names or other personal identifying information, they do not include cell site or other location information, and they do not include the content of any phone calls. These are the kinds of records that under longstanding Supreme Court precedent are not protected by the Fourth Amendment.

The short court order you have seen published in the newspapers only allows the government to acquire the phone records; it does not allow the government to access or use them. The terms under which the government may access or use the records is covered by another, more detailed court order. That other court order provides that the government can only search the data if it has a “reasonable, articulable suspicion” that the phone number being searched is associated with certain terrorist organizations. The order also imposes numerous other restrictions on NSA to ensure that only properly trained analysts may access the data, and that they can only access it when the reasonable, articulable suspicion predicate has been met and documented. The documentation of the analyst’s justification is important so that it can be reviewed by supervisors before the search and audited afterwards to ensure compliance.

In the criminal context, the government could obtain the same types of records with a grand jury subpoena, without going to court. But here, we go to the court approximately every 90 days to seek the court's authorization to collect the records. In fact, since 2006, the court has authorized the program on 34 separate occasions by 14 different judges. As part of that renewal process, we inform the court whether there have been any compliance problems, and if there have been, the court will take a very hard look and make sure we have corrected these problems. As we have explained before, the 11 judges on the FISC are far from a rubber stamp; instead, they review all of our pleadings thoroughly, they question us, and they don't approve the order until they are satisfied that we have met all statutory and constitutional requirements.

In addition to the Judiciary, Congress also plays a significant role in this program. The classified details of this program have been extensively briefed to both the Judiciary and Intelligence Committees and their staffs on numerous occasions. If there are any significant issues that arise with the 215 program, those would be reported to the two committees right away. Any significant interpretations of FISA by the Court would likewise be reported to the committees under our statutory obligation to provide copies of any FISC opinion or order that includes a significant interpretation of FISA, along with the accompanying court

documents. All of this reporting is designed to assist the two committees in performing their oversight role with respect to the program.

In addition, Congress plays a role in reauthorizing the provision under which the government has carried out this program since 2006. Section 215 of the PATRIOT Act has been renewed several times since the program was initiated – including most recently for an additional four years in 2011. In connection with the recent renewals of 215 authority, the government provided a classified briefing paper to the House and Senate Intelligence Committees to be made available to all Members of Congress. That briefing paper set out the operation of the program in detail, explained that the government and the FISC had interpreted section 215 to authorize the bulk collection of telephone metadata, and stated that the government was collecting such information. We also made offers to brief any member on the 215 program. The availability of the briefing paper and opportunity of an oral briefing were communicated through letters sent by the Chairs of the Intelligence Committees to all Members of Congress. Thus, although we could not talk publicly about the program at the time – since its existence was properly classified – the Executive Branch took all reasonably available steps to ensure that members of Congress were appropriately informed about the program when they renewed the 215 authority.

I understand that there have been recent proposals to amend section 215 authority to limit the bulk collection of telephone metadata. As the President has said, we welcome a public debate about how best to safeguard both our national security and the privacy of our citizens. Indeed, we will be considering in the coming days and weeks further steps to declassify information and help facilitate that debate. In the meantime, however, we look forward to working with the Congress to determine in a careful and deliberate way what tools can best secure the nation while also protecting our privacy interests.

Although my opening remarks have focused on the 215 program, we stand ready to take your questions on the 702 program. Thank you.

**NSA OPENING STATEMENT
SENATE JUDICIARY COMMITTEE
OPEN HEARING ON MEDIA LEAKS
31 JULY 2013**

Introduction

Mr. Chairman, Mr. Ranking member, members of the committee, thank you for the opportunity to join with my colleagues to brief the committee on issues **you've identified** in your invitation and opening remarks. I am privileged today to represent the work of thousands of NSA, intelligence community and law enforcement personnel who employ the authorities provided by the combined efforts of the Congress, Federal Courts and the Executive Branch.

For its part, NSA is necessarily focused on the generation of foreign intelligence but we have worked hard and long with counterparts across the US government and allies to **ensure that we "discover and connect the dots"** -- exercising only those authorities explicitly granted to us and taking care to ensure the protection of civil liberties and privacy.

Per your request, I will briefly describe how NSA implements the two NSA programs leaked to the media almost two months ago, to include their purpose and the controls imposed on their use – the so-called PRISM program authorized under section 702 of the FISA amendment act (FAA) and the so-called 215 program which authorizes the collection of telephone metadata.

Let me first say that these programs are distinguished *but complementary* with distinct purposes and oversight mechanisms. Neither of these programs was intended to stand alone, delivering singular results that tell the 'whole story' about a particular threat to our Nation or its allies.

I'll start with **Section 702 of the FISA**, which authorizes the targeting of non-U.S. persons abroad for foreign intelligence purposes such as counter-terrorism and counter-proliferation.

- Specifically, Section 702 authorizes the collection of communications for the purpose of Foreign Intelligence with the compelled assistance of an electronic communication service provider.
- Under this authority NSA can collect communications for foreign intelligence purposes only when the person who is the target of our collection is a foreigner who is reasonably believed to be outside the US.
- Section 702 cannot be used to intentionally target:

- o any US citizen or other US person,
- o any person known to be in the US,
- o OR a person outside the United States if the purpose is to target a person inside the United States

This program is also key to our counterterrorism efforts; information used in greater than 90% of the 54 disrupted terrorism events we have previously cited in public testimony was gained from section 702 authorities.

As one example, **we've** discussed the case of Najibullah Zazi. NSA analysts, leveraging section 702 to target the email of a Pakistan-based al-Qaida terrorist, discovered that he was communicating with someone about a plot involving explosives. NSA tipped this exchange to the FBI who confirmed that the communicant was actually Denver-based Zazi, who we know now was planning an imminent attack on the New York subway system. Without the tip from FAA 702, the plot may never have been uncovered.

The second program, which we undertake through court orders under **Section 215 of the Patriot Act**, authorizes the collection of telephone metadata only.

- **It does not allow the government to listen to anyone's phone calls.**
- This program was specifically developed to allow the USG to detect communications between known or suspected terrorists who are operating outside the U.S. who are communicating with potential operatives inside the U.S., a gap highlighted by the attacks of 9/11. *In a phrase this program is focused on detecting terrorist plots that cross the seam between foreign terrorist organizations and the US homeland.* We have previously cited in public testimony, that section 215 made a contribution to 12 of the 13 terror plots with a US nexus, amongst the 54 world-wide plots cited earlier.

On operational value:

In considering operational value, it is important to begin with an understanding of the problem the government is trying to solve.

- It is simply this: If we have intelligence indicating that a foreign-based terrorist organization is plotting an act of terror against the homeland, how would we determine whether there is, in fact, a connection between persons operating overseas and operatives within the US?
- Many will recall that the inability of the US intelligence community to make such a connection between 9/11 hijacker Al Midhar operating in California and an Al Qaeda safe house in Yemen, which was discussed by the 9/11 commission report.

- NSA had in fact collected the Yemen end of their communications but due to the nature of our collection, had no way of determining the number or the location of Al Midhar on the other end.

So the problem becomes, if you have one telephone number for a person you reasonably believe is plotting an act of terror against the homeland, how do you find possible connections to that number crossing the seam between the homeland and overseas?

In simple terms, you are looking for a needle, *in this case a number*, in a haystack. But not just any number. You want to make a focused query against a body of data that returns only those numbers that are connected to the one you have reasonable suspicion is connected to a terrorist group.

But unless you have the haystack – in this case all the records of who called whom – you cannot answer the question. The confidence you will have in any answers returned by your query is necessarily tied to whether the haystack constitutes a reasonably complete set of records and whether those records look back a reasonable amount of time to enable you to discover a connection between conspirators who might plan and coordinate across several years.

Hence “all” the records are necessary to connect the dots of an ongoing plot, sometimes in a time sensitive situation, even if only an extremely small fraction of them is **ever determined to be the match you’re looking for.**

The authorities work in concert

As I mentioned at the outset, these authorities work together to enable our support to counter-terrorism. A counter-terrorism investigation is the product of many leads, a handful of which may prove to be decisive. It is impossible to know which tool is going to generate the decisive lead in any particular case. In some cases, the leads may corroborate a lead FBI is already following; in others, it may help them prioritize leads for further investigation; in still others it may yield a number that was previously unknown to them. These leads results in threat assessments, preliminary investigations and full investigations; in some cases, the data from the program yields no results, helping to disprove leads and conserve investigative resources. This is the way we would want these programs to work: adding dots, affirming them, connecting them, and in so doing contributing key pieces to the larger intelligence picture.

Using the Zazi case, once FBI confirmed Zazi’s identity, they passed NSA his phone number, for which NSA then made a determination of “Reasonable Articulable Suspicion”, and used the number to search the 215 database. Based on that search NSA analysts discovered a previously unknown number in communication with Zazi for a man named Adis Medunjanin. While FBI had previously been aware of Medunjanin, the direct and recent connection to Zazi as well as another us-based extremist focused

the **FBI's** attention on him as a key lead in the plot. as you know, both Zazi and Medunjanin have been convicted for their role in the plot.

Controls and Limitations:

The limitations and controls imposed on the use of both of these programs are significant.

For the 215 metadata these controls are laid out in the FISA **court's "primary order"** which the executive branch has declassified this morning so that it might provide **context for the court's "secondary order",** leaked earlier in the press, but which only dealt with the collection of the data.

Under rules imposed by the Primary Order:

- The metadata acquired and stored under the 215 authority may be queried only when there is a reasonable suspicion based on specific facts that a **"selector"**—which is typically a phone number—is associated with specific foreign terrorist organizations.
- Under rules approved by the court, only 22 people at NSA are allowed to approve the selectors used to initiate a search in this data base; all queries are audited; only seven positions at NSA (a total of 11 people) are authorized to release query results that are believed to be associated with persons in the US.
- Reports are filed with the court every 30 days that specify the number of selectors approved, and disseminations made to the FBI that contain numbers believed to be in the US.
- And, while the data acquired under this authority might theoretically be useful in other intelligence activities or law enforcement investigations, its use for any **other purpose than that which I've described is prohibited.**

With this capability, we are very mindful that we must use it conservatively and judiciously, in close concert with our law enforcement colleagues and focused on the seam between foreign terrorist groups and potential domestic actors.

- During 2012, we only initiated queries for information in this dataset using fewer than 300 unique selectors. The information returned from these queries only included phone numbers, not the content, identity, or location of the called or calling party. And in 2012, based on those fewer than 300 selectors, we provided a total of 12 reports to FBI, **which altogether 'tipped' less than 500** numbers.

The 702 program operates under equally strict controls that, while ensuring our efforts are focused on the collection of foreign intelligence, specifically address how analysts should handle incidentally collected US person communications.

When NSA targets a terrorist overseas, they may sometimes communicate with persons in the US (anyone in the US, a US citizen or foreign person, is considered a US person). **That's what we call "incidental collection."**

If the case of a communication involving a US person, we have court approved minimization procedures that we must follow.

- This was the case with Najibullah Zazi. As I mentioned, we intercepted that communication using 702 collection by focusing on the Pakistani based al-Qa'ida terrorist.
- While it was not completely clear from the communication who Zazi was or where he was located, NSA analysts immediately tipped this exchange to the FBI who confirmed that Zazi was in fact in Denver and subsequently acquired a warrant to target and access the content of his communications.
- Without that initial 702 tip from NSA, which came as a result of targeting an al-Qa'ida terrorist located overseas, **the plot may never have been discovered.**
- This tip was handled in complete accordance with the applicable minimization procedures which authorized NSA to disseminate information of or concerning a US person if the US person information is necessary to understand or assess foreign intelligence information.
- Finally, NSA cannot reverse target, i.e. target a foreign person overseas if the intent is to target the communications of a person in the US.

We do of course have tools that allow analysts to conduct focused searches of our holdings and listen to the content of legally acquired collection concerning foreign intelligence targets. Given that these communications have been shown to bear on our foreign intelligence mission, we must and do review them. But the purpose is to glean foreign intelligence and the rules for protecting the identities and communications of US persons are both clear and followed.

Looking forward:

Policy makers across the executive and legislative branches will ultimately decide whether we want to sustain or dispense with a tool designed to detect terrorist plots across the seam between foreign and domestic domains. Different implementations of the program can address the need, but each should be scored against several key attributes:

- Privacy concerns must be addressed through controls and accountability;
- It should be possible to make queries in a timely manner so that, in the most demanding case, results can support disruption of imminent plots;
- The database must be reasonably complete across providers and time to yield so that we can have confidence in the answers it yields about whether there is, or is not, a terrorist plot in play; and

- The data architecture is constructed in a manner that allows efficient follow-up queries to any selector that shows connections to other numbers of legitimate relevance to an ongoing plot.

Conclusion

Our primary responsibility is to defend the Nation. The programs we are discussing today are a core part of those efforts. We use them to protect the lives of Americans and our allies and partners worldwide.

Over 100 nations are capable of collecting Signals Intelligence or operating a lawful intercept capability that enable them to monitor communications.

- I think our Nation is amongst the best at protecting our privacy and civil liberties.
- We look forward to the discussions here and, if necessary, at classified sessions to more fully explore your questions BUT I note that the leaks that have taken place thus far will cause serious damage to our intelligence capabilities.
- More to the point, the irresponsible release of classified information will have a long-term detrimental impact on the Intelligence Community's ability to detect and help deter future attacks.
- The men and women of NSA are committed to compliance with the law and the protection of privacy and civil liberties. The solutions they develop and the actions they take defend the Constitution and the American people, both their physical safety and their right to privacy. We train them from their first day at work and throughout their career.
- This is also true of contractors. The actions of one contractor should not tarnish all the contractors because they do great work for our nation, as well.
- Allegations that low level analysts at NSA can exercise independent discretion beyond these controls to target communications is simply wrong.

Finally, whatever further choices the Nation makes on this matter in consultation and collaboration across the three branches of government, NSA will faithfully implement them – in both spirit and mechanism. To do otherwise would be to fail in the only oath we take – to support and defend the Constitution of the United States – to include protection of both National Security and Civil Liberties.



Testimony of

Jameel Jaffer

Deputy Legal Director of the
American Civil Liberties Union Foundation

Laura W. Murphy

Director, Washington Legislative Office
American Civil Liberties Union

Before

The Senate Judiciary Committee

Strengthening Privacy Rights and National Security:
Oversight of FISA Surveillance Programs

July 31, 2013

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 two months 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. These unconstitutional surveillance programs are the product of defects both in the law itself and in the current oversight system. 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.

First, it should amend relevant provisions of FISA to prohibit suspicionless, "dragnet" monitoring or tracking of Americans' communications. Amendments of this kind should be made to the FISA Amendments Act, to FISA's so-called "business records" provision, and to the national security letter authorities.

Second, it should end the unnecessary and corrosive secrecy that has obstructed congressional and public oversight. It should require the publication of FISC opinions insofar as they evaluate the meaning, scope, or constitutionality of the foreign-intelligence laws. It should require the government to publish basic statistical information about the government's use of foreign-intelligence authorities. And it should ensure that "gag orders" associated with national security letters and other surveillance directives are limited in scope and duration, and imposed only when necessary.

Third, it should ensure that the government's surveillance activities are subject to meaningful judicial review. It should clarify by statute the circumstances in which individuals can challenge government surveillance in ordinary federal courts. It should provide for open and adversarial proceedings in the FISC when the government's surveillance applications raise novel issues of statutory or constitutional interpretation. It should also pass legislation to ensure that the state secrets privilege is not used to place the government's surveillance activities beyond the reach of the courts.

Thank you again for the invitation to testify. We appreciate the Committee's attention to this set of issues.

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 to 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

Intelligence officials have said that the government does not “indiscriminately sift through” the phone-record database. Instead, it queries the database “only when there is reasonable suspicion, based on specific and articulated facts, that an identifier is associated with specific foreign terrorist organizations.”⁵ According to a statement released by the government last month, “less than 300 unique identifiers met this standard and were queried” in 2012.⁶ But even if the government ran queries on only 300 unique identifiers in 2012, those searches implicated the privacy of millions of Americans. Intelligence officials have explained that analysts are permitted to examine the call

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>.

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

⁵ See, e.g., *How Disclosed NSA Programs Protect Americans, and Why Disclosure Aids Our Adversaries: Hearing Before the H. Permanent Select Intelligence Comm.*, 113th Cong. (June 18, 2013) (testimony of NSA Deputy Director John C. Inglis), <http://bit.ly/15kZ9wh>.

⁶ See, e.g., Ellen Nakashima, *Call Records of Fewer Than 300 People Were Searched in 2012, U.S. Says*, Wash. Post, June 15, 2013, <http://wapo.st/148Z7Wm>.

records of all individuals within three “hops” of a specific target.⁷ As a result, a query yields information not only about the individual thought to be “associated with [a] specific foreign terrorist organization[]” but about all of those separated from that individual by one, two, or three degrees. Even if one assumes, conservatively, that each person has an average of 40 unique contacts, an analyst who accessed the records of everyone within three hops of an initial target would have accessed records concerning more than two million people.⁸ Multiply that figure by the 300 phone numbers the NSA says that it searched in 2012, and by the seven years the program has apparently been in place, and one can quickly see how official efforts to characterize the extent and impact of this program are deeply misleading.

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.⁹ 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).

⁷ *See* Pete Yost, *Congress Expresses Anger Over NSA Surveillance Program*, Boston Globe, July 18, 2013, <http://b.globe.com/17moqWU>.

⁸ *Id.*

⁹ 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.

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).¹⁰

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.”¹¹

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

¹⁰ 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.

¹¹ 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>.

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.”).¹² The information collected by the government under the metadata program goes far beyond anything a court has ever allowed under the rubric of “relevance.”¹³

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

¹² *See also Hale v. Henkel*, 201 U.S. 43, 76-77 (1906).

¹³ 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.

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 Rep. 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, and another sponsored by Senator Leahy, would also 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 2008.¹⁴ 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.¹⁵ 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.¹⁶ 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.

¹⁴ 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>.

¹⁵ 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.

¹⁶ 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>.

a. Section 702 is unconstitutional

President Bush signed the FISA Amendments Act into law on July 10, 2008.¹⁷ 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

¹⁷ 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 House Judiciary 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>.

§ 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.”¹⁸ 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.

¹⁸ *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>.

The ACLU has long expressed deep concerns about the lawfulness of the FISA Amendments Act and surveillance under Section 702.¹⁹ 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"

¹⁹ 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.

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,²⁰ 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

²⁰ 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>.

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.²¹ 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.

²¹ 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>.

- *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.²² 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.²³ Executive officials testified before Congress several years ago that declassification review was already underway,²⁴ 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.

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. National Security Letters

The ACLU has a number of serious concerns with the national security letter (NSL) statutes. In this testimony, we focus on only two. The first is that the NSL statutes allow executive agencies (usually the FBI) to obtain records about people who are not known or even suspected to have done anything wrong. They allow the

²² See, e.g., Glenn Kessler, *James Clapper's 'Least Untruthful' Statement to the Senate*, Wash. Post, June 12, 2013, <http://wapo.st/170VVSu>.

²³ See Eric Lichtblau, *In Secret, Court Vastly Broadens Powers of N.S.A.*, N.Y. Times, July 6, 2013, <http://nyti.ms/12beiA3>.

²⁴ 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>.

government to collect information, sometimes very sensitive information, not just about suspected terrorists and spies but about innocent people as well. The second concern is that the NSL statutes allow government agencies (again, usually the FBI) to prohibit NSL recipients from disclosing that the government sought or obtained information from them. This authority to impose non-disclosure orders—gag orders—is not subject to meaningful judicial review. Indeed, as discussed below, the review contemplated by the NSL statutes is no more than cosmetic.²⁵

a. The NSL statutes invest the FBI with broad authority to collect constitutionally protected information pertaining to innocent people

Several different statutes give executive agencies the power to issue NSLs.²⁶ Most NSLs, however, are issued by the FBI under 18 U.S.C. § 2709,²⁷ which was originally

²⁵ The ACLU has a number of other concerns with the NSL statutes. First, the statutes do not significantly limit the retention and dissemination of NSL-derived information. *See, e.g.*, 18 U.S.C. § 2709(d) (delegating to the Attorney General the task of determining when, and for what purposes, NSL-derived information can be disseminated). Second, the statutes provide that courts that hear challenges to gag orders must review the government’s submissions *ex parte* and *in camera* “upon request of the government”; this language could be construed to foreclose independent consideration by the court of the constitutional ramifications of denying the NSL recipient access to the evidence that is said to support a gag order. 18 U.S.C. § 3511(e). *But see Doe v. Gonzales*, 500 F. Supp. 2d 379, 423-24 (S.D.N.Y. 2007) (construing statute more narrowly). Third, the statutes provide that courts that hear challenges to gag orders must seal documents and close hearings “to the extent necessary to prevent an unauthorized disclosure of a request for records”; this language could be construed to divest the courts of their constitutional responsibility to decide whether documents should be sealed or hearings should be closed. 18 U.S.C. § 3511(d). *But see Doe*, 500 F. Supp. 2d at 423-24 (finding that statute “in no way displaces the role of the court in determining, in each instance, the extent to which documents need to be sealed or proceedings closed and does not permit the scope of such a decision to be made unilaterally by the government”).

²⁶ For instance, under 12 U.S.C. § 3414(a)(5)(A), the FBI is authorized to compel “financial institutions” to disclose customer financial records. The phrase “financial institutions” is defined very broadly, and encompasses banks, credit unions, thrift institutions, investment banks, pawnbrokers, travel agencies, real estate companies, and casinos. 12 U.S.C. § 3414(d) (adopting definitions in 31 U.S.C. § 5312). Under 15 U.S.C. § 1681u, the FBI is authorized to compel consumer reporting agencies to disclose “the names and addresses of all financial institutions . . . at which a consumer maintains or has maintained an account,” as well as “identifying information respecting a consumer, limited to name, address, former addresses, places of employment, or former places of employment.” Under 15 U.S.C. § 1681v, executive agencies authorized to conduct intelligence or counterintelligence investigations can compel consumer reporting agencies to disclose “a consumer report of a consumer and all other information in a consumer’s file.” Still another statute, 50 U.S.C. § 436 empowers “any authorized investigative agency” to compel financial institutions and consumer reporting agencies to disclose records about agency employees.

enacted in 1986 as part of the Electronic Communications Privacy Act (“ECPA”).²⁸ Since its enactment, the ECPA NSL statute has been amended several times. In its current incarnation, it authorizes the FBI to issue NSLs compelling “electronic communication service provider[s]” to disclose “subscriber information,” “toll billing records information,” and “electronic communication transactional records.”²⁹ An “electronic communication service” is “any service which provides to users thereof the ability to send or receive wire or electronic communications.”³⁰

Because most NSLs are issued under ECPA, this testimony focuses on that statute. All of the NSL statutes, however, suffer from similar flaws.

The ECPA NSL statute implicates a broad array of information, some of it extremely sensitive. Under the statute, an Internet service provider can be compelled to disclose a subscriber’s name, address, telephone number, account name, e-mail address, and credit card and billing information. It can be compelled to disclose the identities of individuals who have visited a particular website, a list of websites visited by a particular individual, a list of e-mail addresses with which a particular individual has corresponded, or the e-mail address and identity of a person who has posted anonymous speech on a political website. As the *Library Connection* case shows, the ECPA NSL statute can also be used to compel the disclosure of library patron records.³¹ Clearly, all of this information is sensitive. Some of it is protected by the First Amendment.³²

Because NSLs can reach information that is sensitive, Congress originally imposed stringent restrictions on their use. As enacted in 1986, the ECPA NSL statute permitted the FBI to issue an NSL only if it could certify that (i) the information sought was relevant to an authorized foreign counterintelligence investigation; and (ii) there were specific and articulable facts giving reason to believe that the subject of the NSL was a foreign power or foreign agent.³³ Since 1986, however, the reach of the law has been extended dramatically. In 1993, Congress relaxed the individualized suspicion requirement, authorizing the FBI to issue an NSL if it could certify that (i)

²⁷ Dep’t of Justice, Office of Inspector General, *A Review of the FBI’s Use of National Security Letters: Assessment of Corrective Actions and Examination of NSL Usage in 2006*, (March 2008), (hereinafter “2008 OIG Report”), at 107, available at <http://1.usa.gov/17PO5aI>.

²⁸ See Pub L. No. 99-508, Title II, § 201(a), 100 Stat. 1848 (Oct. 21, 1986) (codified as amended at 18 U.S.C. § 2510 *et seq.*)

²⁹ 18 U.S.C. §§ 2709(a) & (b)(1).

³⁰ *Id.* § 2510(15).

³¹ See *Library Connection v. Gonzales*, 386 F. Supp. 2d 66 (D. Conn. 2005).

³² Cf. *Mcintyre v. Ohio Elections Comm.*, 514 U.S. 334, 341-42 (1995) (“[A]n author’s decision to remain anonymous, like other decisions concerning omissions or additions to the content of a publication, is an aspect of the freedom of speech protected by the First Amendment.”); *Talley v. California*, 362 U.S. 60, 64 (1960) (“Even the Federalist Papers, written in favor of the adoption of our Constitution, were published under fictitious names.”).

³³ 18 U.S.C. § 2709 (1988).

the information sought was relevant to an authorized foreign counterintelligence investigation; and (ii) there were specific and articulable facts giving reason to believe that *either* (a) the subject of the NSL was a foreign power or foreign agent, *or* (b) the subject had communicated with a person engaged in international terrorism or with a foreign agent or power “under circumstances giving reason to believe that the communication concerned international terrorism.”³⁴ In 2001, Congress removed the individualized suspicion requirement altogether and also extended the FBI’s authority to issue NSLs in terrorism investigations. In its current form, the NSL statute permits the FBI to issue NSLs upon a certification that the records sought are “relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities.”³⁵

The relaxation and then removal of the individualized suspicion requirement has resulted in an exponential increase in the number of NSLs issued each year. According to an audit conducted by the Justice Department’s OIG, the FBI’s internal database showed that the FBI issued 8,500 NSL requests in 2000, the year before the Patriot Act eliminated the individualized suspicion requirement.³⁶ By comparison, the FBI issued 39,346 NSL requests in 2003; 56,507 in 2004; 47,221 in 2005; and 49,425 in 2006.³⁷ These numbers, though high, substantially understate the number of NSL requests actually issued, because the FBI has not kept accurate records of its use of NSLs. The OIG sampled 77 FBI case files and found 22 percent more NSL requests in the case files than were recorded in the FBI’s NSL database.³⁸ Since 2007, the public has had only partial information about the FBI’s use of its NSL authorities. Neither the FBI nor the Department of Justice annually publish the total number of NSLs; instead, the Department of Justice reports statistics that omit NSLs concerning non-U.S. persons and NSLs strictly for subscriber information—making a true comparison impossible. These partial statistics indicate that the FBI issued 16,804 NSLs seeking information concerning U.S. persons in 2007; 24,744 in 2008; 14,788 in 2009; 24,287 in 2010; 16,511 in 2011; and 15,229 in 2012.³⁹

The statistics and other public information make clear that the executive branch is now using NSLs not only to investigate people who are known or suspected to present threats but also—and indeed principally—to collect information about innocent

³⁴ Pub. L. 103-142, 107 Stat. 1491 (Nov. 17, 1993).

³⁵ 18 U.S.C. § 2709(a) & (b)(1) (2006).

³⁶ See Dep’t of Justice, Office of Inspector General, *A Review of the Federal Bureau of Investigation’s Use of National Security Letters* (March 2007), (hereinafter “2007 OIG Report”), at xvi, available at <http://bit.ly/16woHoY>.

³⁷ See *id.* at xix; 2008 OIG Report at 9.

³⁸ 2007 OIG Report at 32.

³⁹ See Electronic Privacy Information Center, *Foreign Intelligence Surveillance Act Court Orders 1979-2012*, May 4, 2012, <http://bit.ly/cnSWP5> (compiling NSL statistics); Kim Zetter, *Federal Judge Finds National Security Letters Unconstitutional, Bans Them*, *Wired*, Mar. 15, 2013, <http://bit.ly/YzEtgG> (same).

people.⁴⁰ News reports indicate that the FBI has used NSLs “to obtain data not only on individuals it saw as targets but also details on their ‘community of interest’—the network of people that the target was in contact with.”⁴¹ Some of the FBI’s investigations appear to be nothing more than fishing expeditions. In two cases brought the ACLU, the FBI has abandoned its demand for information after the NSL recipient filed suit; that is, the FBI withdrew the NSL rather than try to defend the NSL to a judge.⁴² The agency’s willingness to abandon NSLs that are challenged in court raises obvious questions about the agency’s need for the information in the first place.

The ACLU believes that the current NSL statutes do not appropriately safeguard the privacy of innocent people. Congress should narrow the NSL authorities that allow the FBI to demand information about individuals who are not the targets of any investigation.

b. The NSL statutes allow the FBI to impose gag orders without meaningful judicial review

A second problem with the NSL statutes is that they empower executive agencies to impose gag orders that are not subject to meaningful judicial review.⁴³ Until 2006, the ECPA NSL statute categorically prohibited NSL recipients from disclosing to any person that the FBI had sought or obtained information from them.⁴⁴ Congress amended the statute, however, after a federal district court found it unconstitutional.⁴⁵ Unfortunately, the amendments made in 2006, while addressing some problems with the statute, made the gag provisions even more oppressive. The new statute permits the FBI to decide on a case-by-case basis whether to impose gag orders on NSL recipients but strictly confines the ability of NSL recipients to challenge such orders in court.

As amended, the NSL statute authorizes the Director of the FBI or his designee (including a Special Agent in Charge of a Bureau field office) to impose a gag order on

⁴⁰ The statistics also make clear that the FBI is increasingly using NSLs to seek information about U.S. persons. The percentage of NSL requests generated from investigations of U.S. persons increased from approximately 39 percent of NSL requests in 2003 to approximately 57 percent in 2006. 2008 OIG Report at 9.

⁴¹ Eric Lichtblau, *F.B.I. Data Mining Reached Beyond Initial Targets*, N.Y. Times, Sept. 9, 2007; see also Barton Gellman, *The FBI’s Secret Scrutiny: In Hunt for Terrorists, Bureau Examines Records of Ordinary Americans*, Wash. Post, Nov. 6, 2005 (reporting that the FBI apparently used NSLs to collect information about “close to a million” people who had visited Las Vegas).

⁴² See generally *Doe v. Mukasey*, 549 F.3d 861 (2d. Cir. 2008); *Library Connection v. Gonzales*, 386 F. Supp. 2d 66 (D. Conn. 2005).

⁴³ All of the NSL statutes authorize the imposition of such gag orders.

⁴⁴ 18 U.S.C. § 2709 (2005).

⁴⁵ *Doe v. Ashcroft*, 334 F. Supp. 2d 471 (S.D.N.Y. 2004).

any person or entity served with an NSL.⁴⁶ To impose such an order, the Director or his designee must “certify” that, absent the non-disclosure obligation, “there may result a danger to the national security of the United States, interference with a criminal, counterterrorism, or counterintelligence investigation, interference with diplomatic relations, or danger to the life or physical safety of any person.”⁴⁷ If the Director of the FBI or his designee so certifies, the recipient of the NSL is prohibited from “disclos[ing] to any person (other than those to whom such disclosure is necessary to comply with the request or an attorney to obtain legal advice or legal assistance with respect to the request) that the [FBI] has sought or obtained access to information or records under [the NSL statute].”⁴⁸ Gag orders imposed under the NSL statute are imposed by the FBI unilaterally, without prior judicial review. While the statute requires a “certification” that the gag is necessary, the certification is not examined by anyone outside the executive branch. No judge considers, before the gag order is imposed, whether secrecy is necessary or whether the gag order is narrowly tailored.

The gag provisions permit the recipient of an NSL to petition a court “for an order modifying or setting aside a nondisclosure requirement.”⁴⁹ However, in the case of a petition filed “within one year of the request for records,” the reviewing court may modify or set aside the nondisclosure requirement only if it finds that there is “no reason to believe that disclosure may endanger the national security of the United States, interfere with a criminal, counterterrorism, or counterintelligence investigation, interfere with diplomatic relations, or endanger the life or physical safety of any person.”⁵⁰ Moreover, if a designated senior government official “certifies that disclosure may endanger the national security of the United States or interfere with diplomatic relations,” the certification must be “treated as conclusive unless the court finds that the certification was made in bad faith.”⁵¹

In December 2008, the Second Circuit issued a decision construing the NSL statute (1) to permit a nondisclosure requirement only when senior FBI officials certify that disclosure may result in an enumerated harm that is related to “an authorized investigation to protect against international terrorism or clandestine intelligence

⁴⁶ 18 U.S.C. § 2709(c).

⁴⁷ *Id.* § 2709(c)(1).

⁴⁸ *Id.*

⁴⁹ *Id.* § 3511(b)(1).

⁵⁰ *Id.* § 3511(b)(2).

⁵¹ *Id.* In the case of a petition filed under § 3511(b)(1) “one year or more after the request for records,” the FBI Director or his designee must either terminate the non-disclosure obligation within 90 days or recertify that disclosure may result in one of the enumerated harms. *Id.* § 3511(b)(3). If the FBI recertifies that disclosure may be harmful, however, the reviewing court is required to apply the same extraordinarily deferential standard it is required to apply to petitions filed within one year. *Id.* If the recertification is made by a designated senior official, the certification must be “treated as conclusive unless the court finds that the recertification was made in bad faith.” *Id.*

activities”; (2) to place on the government the burden of showing that a good reason exists to expect that disclosure of receipt of an NSL will risk an enumerated harm; and (3) to require the government, in attempting to satisfy that burden, to adequately demonstrate that disclosure in a particular case may result in an enumerated harm.⁵² The court also invalidated the subsection of the NSL statute that directs the courts to treat as conclusive executive officials’ certifications that disclosure of information may endanger the national security of the United States or interfere with diplomatic relations.⁵³

In addition, the Second Circuit ruled that the NSL statute is unconstitutional to the extent that it imposes a non-disclosure requirement on NSL recipients without placing on the government the burden of initiating judicial review of that requirement.⁵⁴ The court held that this deficiency, however, could be addressed by the adoption of a “reciprocal notice” policy.⁵⁵ Under this policy, the FBI must inform NSL recipients of their right to challenge gag orders. If a recipient indicates its intent to do so, the FBI must initiate court proceedings to establish—before a judge—that the gag order is necessary and consistent with the First Amendment.⁵⁶

Consistent with these judicial rulings, the ACLU supports congressional efforts to ensure that “gag orders” associated with national security letters and other surveillance directives are limited in scope, limited in duration, and imposed only when necessary.

V. Summary of recommendations

For the reasons above, Congress should amend relevant provisions of FISA to prohibit suspicionless, “dragnet” monitoring or tracking of Americans’ communications. Amendments of this kind should be made to the FISA Amendments Act, to FISA’s so-called “business records” provision, and to the national security letter authorities.

Congress should also end the unnecessary and corrosive secrecy that has obstructed congressional and public oversight. It should require the publication of FISC opinions insofar as they evaluate the meaning, scope, or constitutionality of the foreign-intelligence laws. It should require the government to publish basic statistical information

⁵² *Doe v. Mukasey*, 549 F.3d 861, 883 (2d. Cir. 2008).

⁵³ *Id.*

⁵⁴ *Id.*

⁵⁵ *See id.*

⁵⁶ A district court in the Northern District of California recently issued a similar decision, finding that the nondisclosure provision of 18 U.S.C. § 2709(c) violates the First Amendment and that 18 U.S.C. § 3511(b)(2) and (b)(3) violate the First Amendment and separation of powers principles. *In re Nat'l Sec. Letter*, No. C 11-02173 SI, 2013 WL 1095417 (N.D. Cal. Mar. 14, 2013). The court enjoined the government from issuing NSLs under section 2709 or from enforcing the nondisclosure provision in that or any other case. *Id.*

about the government's use of foreign-intelligence authorities. And it should ensure that "gag orders" associated with national security letters and other surveillance directives are limited in scope and duration, and imposed only when necessary.

Finally, Congress should ensure that the government's surveillance activities are subject to meaningful judicial review. It should clarify by statute the circumstances in which individuals can challenge government surveillance in ordinary federal courts. It should provide for open and adversarial proceedings in the FISC when the government's surveillance applications raise novel issues of statutory or constitutional interpretation. It should also pass legislation to ensure that the state secrets privilege is not used to place the government's surveillance activities beyond the reach of the courts.

**Statement of Senator Patrick Leahy (D-Vt.),
Chairman, Senate Judiciary Committee,
Hearing on “Strengthening Privacy Rights and National Security:
Oversight of FISA Surveillance Programs”
July 31, 2013**

Today, the Judiciary Committee will scrutinize government surveillance programs conducted under the Foreign Intelligence Surveillance Act, or FISA. In the years since September 11th, Congress has repeatedly expanded the scope of FISA, and given the Government sweeping new powers to collect information on law-abiding Americans – and we must carefully consider now whether those laws have gone too far.

Last month, many Americans learned for the first time that one of these authorities – Section 215 of the USA PATRIOT Act – has for years been secretly interpreted to authorize the collection of Americans’ phone records on an unprecedented scale. Information was also leaked about Section 702 of FISA, which authorizes NSA to collect the communications of foreigners overseas.

Let me make clear that I do not condone the way these and other highly classified programs were disclosed, and I am concerned about the potential damage to our intelligence-gathering capabilities and national security. We need to hold people accountable for allowing such a massive leak to occur, and we need to examine how to prevent this type of breach in the future.

In the wake of these leaks, the President said that this is an opportunity to have an open and thoughtful debate about these issues. I welcome that statement, because this is a debate that several of us on this Committee have been trying to have for years. And if we are going to have the debate that the President called for, the executive branch must be a full partner. We need straightforward answers and I am concerned that we are not getting them.

Just recently, the Director of National Intelligence acknowledged that he provided false testimony about the NSA surveillance programs during a Senate hearing in March, and his office had to remove a fact sheet from its website after concerns were raised about its accuracy. I appreciate that it is difficult to talk about classified programs in public settings, but the American people expect and deserve honest answers.

It also has been far too difficult to get a straight answer about the *effectiveness* of the Section 215 phone records program. Whether this program is a critical national security tool is a key question for Congress as we consider possible changes to the law. Some supporters of this program have repeatedly conflated the efficacy of the Section 215 bulk metadata collection program with that of Section 702 of FISA. I do not think this is a coincidence, and it needs to stop. The patience and trust of the American people is starting to wear thin.

I asked General Alexander about the effectiveness of the Section 215 phone records program at an Appropriations Committee hearing last month, and he agreed to provide a classified list of terrorist events that Section 215 helped to prevent. I have reviewed that list. Although I agree that it speaks to the value of the overseas content collection implemented under Section 702, it

does not do the same with for Section 215. The list simply does not reflect dozens or even several terrorist plots that Section 215 helped thwart or prevent – let alone 54, as some have suggested.

These facts matter. This bulk collection program has massive privacy implications. The phone records of all of us in this room reside in an NSA database. I have said repeatedly that just because we have the ability to collect huge amounts of data does not mean that we *should* be doing so. In fact, it has been reported that the bulk collection of Internet metadata was shut down because it failed to produce meaningful intelligence. We need to take an equally close look at the phone records program. If this program is not effective, it must end. And so far, I am not convinced by what I have seen.

I am sure that we will hear from witnesses today who will say that these programs are critical in helping to identify and connect the so-called “dots.” But there will always be more “dots” to collect, analyze, and try to connect. The Government is already collecting data on millions of innocent Americans on a daily basis, based on a secret legal interpretation of a statute that does not on its face appear to authorize this type of bulk collection. What will be next? And when is enough, enough?

Congress must carefully consider the powerful surveillance tools that we grant to the Government, and ensure that there is stringent oversight, accountability, and transparency. This debate should not be limited to those surveillance programs about which information was leaked. That is why I have introduced a bill that addresses not only Section 215 and Section 702, but also National Security Letters, roving wiretaps, and other authorities under the PATRIOT Act. As we have seen in the case of ECPA reform, the protection of Americans’ privacy is not a partisan issue. I thank Senator Lee and others for their support of my FISA bill, and hope that other Senators will join our efforts.

Today, I look forward to the testimony of the Government witnesses and outside experts. I am particularly grateful for the participation of Judge Carr, a current member of the judiciary and a former judge of the FISA Court. I hope that today’s hearing will provide an opportunity for an open debate about the law, the policy, and the FISA Court process that led us to this point. We must do all that we can to ensure our nation’s security while protecting the fundamental liberties that make this country great.

#####