Oversight Hearing on the Administration's use of FISA Authorities

Committee on the Judiciary

United States House of Representatives

July 17, 2013

Statement of Stewart A. Baker

Partner, Steptoe & Johnson LLP

Mr. Chairman, Ranking Member Conyers, 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, the government is "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 carrier[10]). 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.

Actually, they didn't just want to spur debate; they tried to control it – by withholding information from the public. If you're an American concerned about government collection of data, slides that talk about large-scale collection direct from private databases are bound to raise concern, especially after release of the phone metadata order. But many of those concerns can be answered by reading the very detailed and strict minimization and targeting guidelines adopted by Justice and the DNI and approved by the FISA court for this program. The whole point of those guidelines is to make sure that NSA's collection protects the privacy of Americans while still allowing foreign intelligence collection to go forward.

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 flap 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

[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

data misuse, that flag questionable searches, and that require employees to explain why they are seeking unusual data access. That's far more likely to provide effective protection against misuse of private data than trying to keep cheap data out of government hands. The federal government has in fact made progress in this area; that's one reason that the minimization and targeting rules could be as detailed as they are. But it clearly needs to do better. A proper system for auditing access to restricted data would not just improve privacy enforcement, it likely would have flagged both Bradley Manning and Edward Snowden for their unusual network browsing habits.

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

---

used ensure accountability for network users. These two safeguards—permissioning and auditing—will free participants to take initiatives within the parameters of our country's legal, cultural, and societal norms.

MARKLE FOUNDATION TASK FORCE, PROTECTING AMERICA'S FREEDOM IN THE INFORMATION AGE 17 (October 2002), http://www.markle.org/sites/default/files/nstf_full.pdf.

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]

Some of this is just hypocrisy. Shortly after President Hollande demanded that the U.S. "immediately stop" its intercepts[13] 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]

---

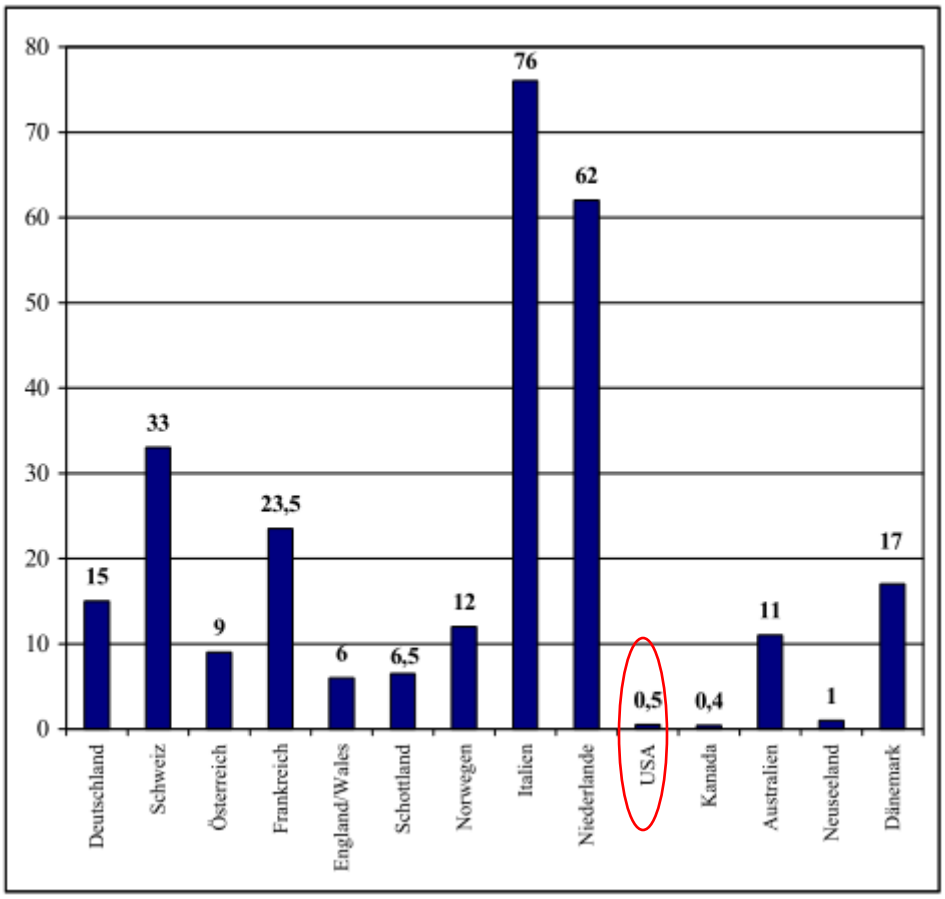
[12] European Parliament resolution of 4 July 2013 on the US National Security Agency surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' privacy (2013/2682(RSP)) at http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P7-TA-2013-0322&language=EN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

[13] Sébastian 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-hypocritcal.

[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. Two lessons are particularly salient as a result of the latest flap over Edward Snowden's revelations.

First, as technologies and security problems change, it is not easy for the law to keep up – at least not without the kind of debate and legislative specification that puts sources and methods at risk. The solution of the past decade has been to erect many safeguards for civil liberties, but behind a veil of classification. The end result has been discouraging. Not because civil liberties have been eroded in secret; in my view, all three branches of government have bent over backwards to protect the privacy of Americans while still conducting intelligence on the frontier of technology. Rather, it's clear that large parts of the body politic are reluctant to trust classified protections. That has allowed irresponsible advocates to distort the debate over our intelligence programs.

Second, we are not alone when we write these laws. Every other country – and practically every terror group – is listening and sifting our debate for clues about what it means for them. The very things that we are proudest of – our ability to conduct intelligence while protecting the rights of Americans – is no comfort to the rest of the world. Instead, it looks to many in the rest of the world like a provocation. They feel entitled to demand for their citizens the protections we have given to Americans. In pursuit of that goal, we can expect them also to attack the technology companies that are at the heart of our competitive and our intelligence advantage. If nothing else, we need to make sure that other governments do not punish those companies for the contribution they make to our security.