Testimony of Stewart A. Baker

Before the Permanent Select Committee on Intelligence
United States House of Representatives

"Potential Amendments to the Foreign Intelligence Surveillance Act"

October 29, 2013

Chairman Rogers, Ranking Member Ruppersberger, members of the committee, it is a great honor to testify before you today on the issues raised by the Snowden leaks. I was the General Counsel of the National Security Agency in the early 1990s, under both George H.W. Bush and Bill Clinton. I have closely followed NSA issues as a private lawyer, as general counsel of the Robb-Silberman Commission on intelligence failures involving Iraq and weapons of mass destruction, and as an author and blogger.

It seems to me that the issues raised by the Snowden disclosures fall into two categories. The first is a topic that has received less attention from Congress but one that poses the greatest threat to the country's security. That is the current campaign by Glenn Greenwald and others who control the Snowden documents to cause the greatest possible diplomatic damage to the United States and its intelligence capabilities.

I fear that this international campaign has forced the executive branch into a defensive crouch. Other nations are taking advantage of the moment to demand concessions that the White House is already halfway to granting. If so, we will regret them as a country long after the embarrassment of fielding angry phone calls from national leaders has faded into a short passage in President Obama's memoirs.

It is time for Congress to look more closely at the long-term security interests of the country and to set limits on the intelligence concessions that other nations demand and that the Executive can make. I will explain why in the first part of my testimony.

The second issue is more familiar. The domestic fallout from the Snowden leaks has been concentrated heavily on NSA's collection of telephone metadata under section 215 of the USA PATRIOT Act. A lot of changes have been proposed in response. Most of them are bad ideas.

But there are bad ideas and worse ones. In the second part of my testimony, I will explain why I think the NSA collection is justified and why the reaction is not. I'll then offer thoughts on which of the reform proposals will do the least harm and which the most.

1. International intelligence gathering

The harder problem at the moment, the one we haven't come close to solving, stems from the fact that Americans aren't the only people following the debate over intelligence collection. 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 may be receding in this country, the storm is still gathering abroad.

Foreign intelligence is crucial

Attacks on NSA's collection of intelligence on foreign governments outside the United States are new. And it's important for the American people to understand how critical NSA's foreign intelligence collection is to our ability to influence events and to protect our people around the world. NSA's ability to track terrorists abroad has been crucial to the degradation of al Qaeda's central command. Terrorists come from every nation, and we cannot offer a refuge in the name of privacy. After all, the attacks of 9/11 were planned in Hamburg, Germany. NSA's aggressive pursuit of terrorists has also paid dividends for other nations with less advanced capabilities – including some of those countries complaining loudest.

But we don't need foreign intelligence capabilities just to track terrorists. The world is full of nations whose interests conflict with ours. Indeed, it is hard to find a country whose interests do not at least occasionally diverge from our own. When that happens, we can expect the other country to do everything it can to help itself and its citizens at the expense of ours. Other countries may protect well-connected criminals or terrorists who victimize Americans; they may help their companies break the trade embargo on Iran; they may be planning to cut off crucial commodity or technology shipments to the United States; they may be getting ready to attack another country or to conduct a genocide; they may be engaged in negotiations over issues from peace in the Middle East to arms control. In every case, our ability to respond to surprises around the globe depends on gathering intelligence on other countries' plans.

We cannot afford to exempt countries that often see themselves as allies from the possibility of intelligence collection. Our interests often diverge from those of even generally friendly countries. Even allies can have bitter disputes, where every bit of information may be needed to ensure a favorable outcome. To take one example, the European Union is filled with NATO allies, but that has not kept Brussels from using hard-nosed tactics to disadvantage U.S. industry and to obstruct important U.S. diplomatic goals on a regular basis.

Equally, we cannot restrict our intelligence community to gathering "what we need, not what we can." Intelligence is not a like electricity, available on demand. It can take years to get into position to collect intelligence – and more years before the intelligence is needed. But when it is needed, the need is often unexpected and urgent, and the years of painstaking effort to gather "what we can" are suddenly worthwhile.

I recognize the diplomatic harm that the Snowden leaks and their orchestration by Glenn Greenwald have caused. 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. The European Parliament has threatened to suspend law enforcement and intelligence agreements.[1] German Chancellor Angela Merkel has personally called President

[1] European Parliament resolution of 4 July 2013 on the US National Security Agency surveillance programme,

Obama to extract an assurance that her phone is not now being targeted. Germany and France have demanded a new international agreement to stop spying between allies.

European hypocrisy

Some of this is just hypocrisy. Shortly after President Hollande demanded that the United States "immediately stop" its intercepts[2] 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.[3] According to French Foreign Minister Bernard Kouchner, "Let's be honest, we eavesdrop, too. Everyone is listening to everyone else. But we don't have the same means as the United States, which makes us jealous."

And let's not forget that Chancellor Merkel visited China right after public disclosures that the Chinese had penetrated her computer network, yet she managed to be "all smiles" for the Chinese while praising relations between the two countries as "open and constructive."[4] There were no calls for sanctions or agreements to put an end to China's notorious hacking campaign.

What's more, 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 over a hundred times more likely to be wiretapped by his government than an American.[5]

---

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

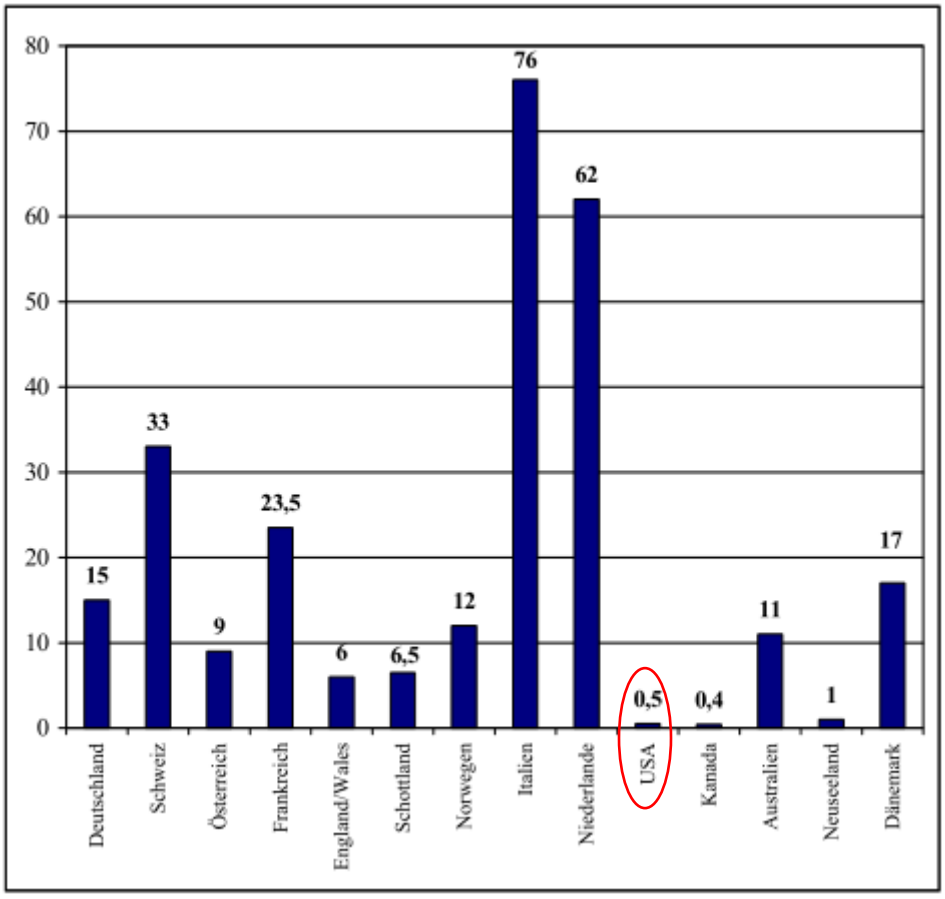
2 Sébastian Seibt, *France's 'hypocritical' spying claims 'hide real scandal'*, FRANCE24 (July 3, 2013), http://www.france24.com/en/20130702-france-usa-spying-snowden-hollande-nsa-prism-hypocritcal (last visited Oct. 28, 2013).

3 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 (last visited Oct. 28, 2013).

4 *See Espionage Report: Merkel's China Visit Marred by Hacking Allegations*, DER SPIEGEL (Aug. 27, 2007), http://www.spiegel.de/international/world/espionage-report-merkel-s-china-visit-marred-by-hacking-allegations-a-502169.html (last visited Oct. 28, 2013).

5 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 (last visited Oct. 28, 2013).

Which countries do the most surveillance per capita?



European regimes, by and large, offer also 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.[6]

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

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

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. Indeed, when one Ars Technica reporter who believed the European hype about its privacy rules took a closer look at European webmail providers, disillusionment set in fast.[7] He found that, unlike their US counterparts, German email providers are unable to issue transparency reports of the sort that US companies have been publishing:

[7] *See* Cyrus Farivar, *Europe won't save you: Why e-mail is probably safer in the US*, ARS TECHNICA (Oct. 13, 2013, 5:00 pm), http://arstechnica.com/tech-policy/2013/10/europe-wont-save-you-why-e-mail-is-probably-safer-in-the-us/2/.

> German law forbids providers to talk about inquiries for user data or handing over user data ... We are currently investigating a possible way with our lawyer to issue a transparency report about questions from police like Google, Microsoft, and [many] other US providers do, but we can not promise we will be able to do so. We try hard.

In addition, while US authorities can get a specific "gag" order to prevent subscribers from knowing that their mail has been seized; the orders can be challenged and often expire on their own. It appears that in Europe disclosure is not an option:

> [A]n American provider could notify its customer that he or she is the target of a judicial investigation. Google has a user notification policy, for instance, that stands unless the court forbids it from disclosing that information. ... German court orders, by contrast, appear to be sealed automatically.

And finally, it appears that European mail providers cannot challenge government discovery orders before turning over the data. In Germany and the Netherlands, the only jurisdictions the writer examined, providers turn over the data first, and then argue about whether they should have to do so. One supplier said that it:

> could challenge a secret court order after the fact, unlike in the case of the United States, where such challenges can be made before such a handover. "If we think the order was not right, we can complain afterwards—and we would do so."

Finally, the European Union, which is threatening to abrogate the SWIFT financial terrorism information sharing agreement, stands in a class by itself for hypocrisy. For more than fifty years, Brussels has watched as the French government spied on other European nations, and as those nations returned the favor, without ever proposing to stop the snooping. It doesn't even have a serious set of data protection rules for the law enforcement agencies of Europe, despite surveillance levels up to 100 times what we experience in the United States. It's true that, 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 and retain their own metadata databases so that law enforcement and security agencies could conveniently search up to two years' worth of logs.[8] 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" disclosures and automatic gag orders) at the request of any government agency anywhere between Bulgaria and Portugal. Yet that abysmal track record on privacy has stopped the European Parliament from declaring its immediate intent to regulate *American* surveillance.

The threat to American intelligence capabilities

[8] *See* Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32006L0024:EN:HTML (last visited Oct. 28, 2013).

Just because much of the outrage around the world is manufactured does not mean that it is without risk for the United States. Quite the contrary, European and other nations see the prospect for enormous gains at the expense of the U.S., in part because President Obama seems genuinely embarrassed and unwilling to defend the National Security Agency. Instead, he is offering assurances to select world leaders that they are not targets, and his homeland security adviser is declaring that "the president has directed us to review our surveillance capabilities, including with respect to our foreign partners. We want to ensure we are collecting information because we *need* it and not just because we *can* [and that] we are balancing our security needs with the privacy concerns all people share."[9] Administration sources have begun criticizing the NSA for putting the President in this bind, and they are hinting at the possibility of negotiating reciprocal deals with other countries that will bar espionage directed at each other while sharing intelligence.

Meanwhile 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."[10] 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."[11] 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."[12]

I suspect that the rest of the world sees an opportunity for a kind of "three-fer" in trying to force companies to store data in France or Germany or Brazil rather than the United States. First, local data storage means more data storage jobs and investment at home and less in the United States. Second, it means that the data (including data about Americans) will be easily available to French and German and Brazilian investigators – without legal process. And third, it makes the United States intelligence agencies weaker and more dependent on the cooperation of Europeans – creating another bargaining chip like the SWIFT arrangement that Europe is already using as leverage in the current flap.

---

[9] Lisa Monaco, *Obama administration: Surveillance policies under review*, USA TODAY (Oct. 24, 2013, 8:43 pm), http://www.usatoday.com/story/opinion/2013/10/24/nsa-foreign-leaders-president-obama-lisa-monaco-editorials-debates/3183331/ (last visited Oct. 28, 2013)

[10] 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/ (last visited Oct. 28, 2013).

[11] *German minister: Drop US sites if you fear spying*, ASSOCIATED PRESS (July 3, 2013), http://www.usatoday.com/story/news/world/2013/07/03/nsa-germany-snowden-websites/2487125/ (last visited Oct. 28, 2013).

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

What Congress Can Do

In short, we face the prospect of two serious attacks on U.S. interests as a result of the Snowden leaks. First, foreign nations will threaten our companies in the hope of moving data and jobs out of the United States. Second, they will capitalize on President Obama's defensive crouch to extract diplomatic and intelligence concessions that would have been unthinkable a year ago.

At the same time, I note, these nations have asked China, which is subjecting them to the most notorious and noisy computer hacking campaign on the planet, for, well, for nothing at all. The reason for that reticence is simple. They know that China will give them nothing.

And that, it seems to me, is where Congress comes in. Sometimes an American negotiator's best friend is an unreasonable Congress. As far as European negotiators are concerned, the United States Congress is almost in China's league. If Congress sets limits on what the executive branch can concede to its foreign counterparts, those limits will be observed. And if Congress specifies consequences for threatening U.S. industry, threatening U.S. industry will be much less attractive.

That's why I suggest that any legislation addressing the domestic intelligence program also address the international campaign to weaken U.S. intelligence capabilities. What would that legislation say? Let me suggest a few possibilities, any one of which would provide U.S. negotiators with useful limits and leverage:

- A "cooling off" provision requiring that any intelligence reciprocity agreement with any nation be submitted to Congress for review prior to taking effect.

- A "start with common ground" provision prohibiting reciprocal intelligence talks with any nation unless the DNI determines that the nation does not use its intelligence services to steal commercial information from private American companies for the benefit of its own companies.

- A "true reciprocity" provision requiring an independent report to this committee from the CIA, NSA, and other agencies prior to any proposed intelligence reciprocity arrangement taking effect; no such arrangement could take effect without a determination by Congress that the arrangement provided benefits to the U.S. intelligence community that matched the benefits to the counterpart nation.

- A "trust but verify" provision requiring that the DNI certify that any reciprocal "no spying" promise in an international agreement be verifiable and enforceable.

- A "no hostage-taking" provision that bars negotiations – and counterterrorism intelligence-sharing – with any European Union member if the European Union terminates its existing terrorism information sharing arrangements with the United States or takes action to punish U.S. companies in an effort to regulate U.S. intelligence or law enforcement agencies. Exceptions for intelligence sharing would require a determination

by the DNI that the sharing is in the national interest of the United States and that the country in question took action to oppose the termination.

- A "stay in your lane" provision barring any negotiation with the European Union that touches on intelligence. The European Union has no authority over European intelligence, and its role in past counterterrorism negotiations has been uniformly hostile to American interests.

- A "sauce for the goose" provision requiring declassified reports from the intelligence community on (1) the scope and intrusiveness of other nations' surveillance of American officials, businessmen, and private citizens and (2) how much data about individual Americans is being retained by companies in Europe and elsewhere, how often it is accessed by European governments, and whether that access meets our constitutional and legal standards.

2. Domestic intelligence-gathering and the telephone metadata program

Why the program makes sense

NSA's telephone metadata program was intended to cure one of the failings of our intelligence community in the run-up to 9/11. NSA intercepted calls that one of the hijacking ringleaders, Khalid al Mihdhar, made from San Diego to a known al Qaeda number in Yemen. But NSA did not have an easy way to determine that the hijacker was already in the United States. That crucial fact would not be discovered until a few weeks before the attacks.

The metadata program filled a gap in our defenses that had cost three thousand lives. It collected a very large amount of information. Taken out of context – and Snowden and Greenwald worked hard to make sure it *was* taken out of context by withholding the minimization guidelines from their readers for two weeks – this was a troubling disclosure. But the minimization guidelines that the journalists withheld show that collecting data isn't the same as actually looking at it. Under the minimization rules, metadata could only be examined by one of two dozen NSA analysts, and they had to supply specific, articulable facts to justify the suspicious nature of the number they wanted to check. In fact the minimization rules were interpreted so strictly that last year the agency only actually looked at records for 300 subscribers and after looking at their records, the agency only passed 500 numbers to the FBI for investigation and identification of the subscriber.[13]

Much of the argument about whether the program was lawful has died down as the rationale approved by the FISA court has become public, and I will leave that issue to Steve Bradbury. I do want to talk about the policy basis for the program. In the absence of the metadata collection, tracing a phone number's contacts would require access to several carriers' records. The effort would be limited by how long the different carriers choose to keep their data, and hampered by

[13] Dana Priest, *Piercing the confusion around NSA's phone surveillance program*, THE WASHINGTON POST (Aug. 8, 2013), http://articles.washingtonpost.com/2013-08-08/world/41198127_1_phone-records-phone-surveillance-program-metadata-program (last visited Oct. 28, 2013).

the different data storage systems they use. It would also be less secure, since every number of interest would have to be sent to every carrier that keeps billing records, including many foreign companies supplying "virtual networks" in the United States. The safest and the fastest way to search the data is to put it in one place.

As long as the rules about access are observed, the end result of the collection-first approach is much the same as a standard law enforcement inquiry, and often it is better. In the standard inquiry, the government establishes the relevance of its inquiry first and is then allowed to collect and search the data. In the new collection-first model, the government collects the data first and then must establish the relevance of each inquiry before it's allowed to conduct a search. In fact, the standard approach almost always sweeps up irrelevant as well as relevant data, and once it has been collected, that data can be searched without limit.

I know it's fashionable to say that letting the government collect all that data could lead to abuses if later administrations change the rules. In fact, 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 about what it wants and why, and you have to count on the court to apply the rules. If you don't trust them to do their job, 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 over a million telephone billing records a year using nothing but a subpoena.[14] 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[15]). 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, we'd be there by now, and without any help from NSA's 300 searches.

How can the program be reformed?

In my view the minimization procedures are working. If anything, the government did too good a job in thinking of restrictions that could be imposed on the program. It is hard to add more without hurting the program's effectiveness. Nonetheless, I recognize the reality that something more must be done if the program is to survive. So I offer below some thoughts on the kinds of reforms now under consideration.

---

[14] 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. Markey Letters to Wireless Carriers on Enforcement Requests, http://www.markey.senate.gov/Markey_Letters_to_Wireless_Carriers.cfm (last visited Oct. 28, 2013).

[15] Letter from Timothy P. McKone, Exec. Vice President, AT&T, to Congressman Edward J. Markey (May 29, 2012), *available at* http://www.markey.senate.gov/documents/2012-05-22_ATT_CarrierResponse.pdf.

"Roamer" authority. Of all the proposals for reform currently being advanced, the best is the proposal to cut NSA some slack when a foreign target unexpectedly shows up in the United States, thus triggering all the legal protections applicable on US soil. It's often difficult for the agency to know that a number is calling from the United States, but today the NSA has to report itself as having violated those rules every time a target makes a call while changing planes in New York or Miami. That is by far the largest category of "violation" that has been used by opponents as evidence that the agency does not obey the law. Rather than set the agency up for an entirely predictable fall, the law should give it time to seek FISA court approval when it finds a foreign target suddenly communicating from the United States, just as we allow emergency FISA taps without court approval for a limited period of time.

Oversight. One of the most troubling aspects of the Snowden affair was the airy dismissal by opponents of the elaborate set of internal controls on intelligence abuses that were erected after the Church and Pike investigations of the 1970s. In an effort to show for the first time that intelligence could be conducted effectively under law and with oversight, Congress created intelligence oversight committees, the FIS court, and a host of internal review authorities such as inspectors general. All of these institutions have top security clearances and independence from the intelligence community. This "1970s model" has been followed for decades, gradually growing stricter. Everyone in Washington accepted it because it seemed the only way to have independent scrutiny of the intelligence community without revealing sensitive programs.

Yet large swaths of the public now dismiss the 1970s model out of hand. These critics didn't have much to offer in its place, other than a vague notion that we need a detailed public debate over every intrusive intelligence program so that every member of Congress and every citizen can weigh in. That won't work. But there is deep public skepticism about allowing the intelligence committees and the court to serve as proxies for the public. Given those doubts, the public may not be much reassured by measures strengthening the independence of the NSA inspector general, say, or tweaking the way the judges of the FIS court are appointed. What's more, as I discuss later, the costs of further expanding the FIS court's role are growing.

Section 215. We cannot play "pick-up sticks" with national security, removing first one and then another of the protections adopted in the wake of 9/11, waiting to see which move actually causes the structure to collapse. The section 215 metadata program was a direct response to the 9/11 attacks, and it is fair to ask opponents of the program how they would close the gap revealed by Khalid al Mihdhar's phone call to Yemen. There may be ways to tighten the program while still protecting the seam between domestic and international intelligence collection, but the burden of doing so should be on proponents.

Some propose to rely on the phone companies to store and produce the data now stored by NSA. I doubt that such a solution would be affordable. It certainly would not be efficient. Nor would it be particularly private, since any metadata stored with the carriers would be subject to subpoena not just by the government but by every divorce lawyer in the country.

FIS Court. Proposals to appoint a special counsel to argue against the government in the FIS court run into the same problem of public trust as the rest of the 1970s model. Anyone whom the court could appoint will have to have a security clearance and intimate familiarity with NSA's

programs. They will need a cleared staff and clerical assistance in classified facilities. They will be, for all intents and purposes, a part of the U.S. government and dependent on the government to function. This will be pointed out by critics every time the court ends up ruling for the government. So setting up yet another advocate against aggressive intelligence gathering isn't likely to restore public trust.

But it will create an imbalance in advocacy. If anything, there are already too many offices competing for the job of protecting citizens' privacy by limiting NSA's capabilities. The NSA inspector general and general counsel see that as part of their jobs, as do the various privacy and civil liberties officers for the intelligence community and the administration as a whole. On top of that, the FISA process has yet another set of officials charged with second-guessing NSA on privacy and law. The Department of Justice sees itself not as the agency's advocate but as a kind of umpire, responsible for balancing privacy and security independent of the agency. The staff attorneys at the FIS court also see themselves playing a significant role in protecting privacy rights. They apparently review and negotiate over FISA warrant applications before they reach the judges, who provide a third layer of umpiring. Every one of these levels of review, I think it's safe to say, is more inclined to trim, condition, and restrict than to expand the searches that NSA proposes.

The justification for having all these umpires is that there's no one on the other side to challenge NSA's requests. But if we're now going to appoint an advocate to argue against the agency's requests, we ought to let the agency argue *for* its requests. As any Red Sox fan will tell you, when the other team takes the field, the umpires should let both teams play. One team should not have three umpires on its side too. So any effort to make the FIS court more truly adversarial should work both ways; NSA should be allowed to file directly in the FIS court and to decide which rulings to appeal.

If there is a problem at the FIS court, it is not the lack of an advocate on the other side. Rather it is the odd, quasi-managerial role we keep pressing on the FIS court. It leaves the court in an awkward spot. The court has been widely criticized as a rubber stamp, and it's clear that the criticism stings. It recently announced that it was keeping statistics to show how often it forces modifications of FISA orders.[16] This raises questions about its even-handed application of the law. Would you want to be judged by a court that goes out of its way to publicize a scorecard of how often it rules against you?

What's more, because the court is so intimately involved in the agency's affairs, the court comes to feel that it has responsibility for the details of how its orders are administered but only limited tools to fulfill that responsibility. Unlike real managers, who have many administrative tools to make sure their policies are carried out, the FIS court has only two: legal rulings and contempt findings. As the court becomes more familiar with the agency, it grows more invested in the implementation of particular measures and policies. The temptation to declare these measures legally necessary is very great. Similarly, when the court is disappointed or surprised by the

[16] *See* Letter from the Honorable Reggie B. Walton, Presiding Judge, the United States Foreign Intelligence Surveillance Court, to the Honorable Charles E. Grassley, Ranking Member, Committee on the Judiciary, United States Senate (Oct. 11, 2013), *available at* http://www.uscourts.gov/uscourts/courts/fisc/ranking-member-grassley-letter-131011.pdf.

agency's implementation of the measures, the temptation to reach for the contempt power is strong. That was certainly true of Presiding Judge Lamberth, who spent most of 2001 pursuing sanctions on a well-regarded FBI agent for not observing the "wall" between law enforcement and intelligence. The judge was so aggressive in this pursuit that the FBI was unable to use its most effective counterterrorism teams to find the al Qaeda plotters whom we learned were in the country in August of 2001. The court of appeals ultimately found the wall to be utterly without a basis in law but by then it was too late. That may be the most egregious misstep by the FIS court, but it is symptomatic of an institutional canker that has recurred under other presiding judges as well.

In the long run, I fear it will become clear that we have given Article III judges responsibilities that belong to the executive branch, and that we will pay another price for that mistake like the one we paid in 2001. For those reasons, I look with great skepticism on expansions of the FIS court's role and discretionary powers, including the authority to bring in outside advocates of its choosing and the authority to appoint an independent and largely permanent staff of lawyers who are bound to develop their own policy views on the intelligence community.

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. Domestic and international forces are pushing the United States toward a new understanding of how to govern our intelligence capabilities. If we make the wrong decisions in the next few months, our intelligence capabilities may be handicapped for a generation – or until some disaster reveals our errors in stark relief.

The responsibility for those choices falls on the President -- and on this committee.