Testimony of Stewart A. Baker

Before the Senate Judiciary Committee

"Continued Oversight of U.S. Government Surveillance Authorities"

November 21, 2013

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.

Intelligence Gathering Under Law

If you'll indulge me, I'd like to start by putting this issue in perspective. Because the fact is that we are engaged in a uniquely American and fairly recent experiment – trying to write detailed legal rules to govern the conduct of foreign intelligence. This is new, even for a country that puts great faith in law. And to be candid, we don't yet know whether the experiment will succeed.

The Americans who fought World War II and much of the Cold War didn't think it would. They believed that intelligence should be insulated from all 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.[1] The military successes that followed made the officers look like heroes, not felons.

That view held for nearly forty years, but it broke down in the wake of Watergate, when Congress took a close look at the intelligence community, found abuses, and in 1978 adopted the first detailed legal regulation of intelligence gathering in history – the Foreign Intelligence Surveillance Act.[2]

---

[1] DAVID KAHN, THE CODEBREAKERS: THE COMPREHENSIVE HISTORY OF SECRET COMMUNICATION FROM ANCIENT TIMES TO THE INTERNET 12 (2d ed. 1996).

[2] 50 U.S.C. Ch. 36.

No other nation has ever tried to regulate intelligence so publicly and so precisely in law. Now, this Committee is considering whether and how to expand the scope and detail of that law.

The Challenges of Intelligence Under Law

Let's start by acknowledging just how hard it is to write laws to govern intelligence. The fundamental problem is that good intelligence operations must be kept secret. The more we disclose about our techniques, the less likely we are to succeed. Much as we might like to get the buy-in of every American or every member of Congress for particular operations, we can't do that. Because intelligence targets pay very close attention to our debates, hoping to learn ways to defeat the techniques that the debates expose.

And, unfortunately, the more we try to regulate intelligence gathering in law, the more techniques we put at risk.

In part that's because law changes slowly while technology changes quickly. So Congress has to change the law frequently just to keep pace. 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 adversaries 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.

That's the first challenge that our experiment in writing intelligence law must overcome.

The second is perhaps more subtle, but it has been costly. We have inserted the Foreign Intelligence Surveillance Court, or FISC, into the heart of our intelligence gathering process, and we have tempted the FISC judges to take on something close to operational responsibilities. This is not their strong suit. Indeed, it's a role that runs counter to their constitution – and to ours.

I will talk about the proposals for intelligence reform in the context of these two challenges.

1. Section 215 and "Collection-First" Safeguards

To be honest, I was initially surprised by the disclosure 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 Edward Snowden worked hard to make sure it *was* taken out of context – this was a troubling disclosure.

NSA's Searches of Phone Metadata Are Strictly Controlled

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 minimization rules designed to make sure that government officials only look at relevant records."[3] Under the minimization rules, metadata can only be examined by one of two dozen NSA analysts, and they have to supply specific, articulable facts to justify the suspicious nature of the number they want to check. In fact the minimization rules have been 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.[4]

NSA's Program Is Legal

By now, I think that most lawyers understand that the program was consistent with law. The Supreme Court has held that billing records are not protected by the Fourth Amendment, because they've already been given to a third party.[5] 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.[6] Several FISC judges examined the program and its legal rationale. All upheld it.

---

[3] 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).

[4] 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 Nov. 20, 2013).

[5] *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)).

[6] *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

The Policy Grounds for NSA's Program

The real question, then, is whether the program *should* be legal. You have before you a bill that would make it illegal, or at least so tilt the playing field that it would likely be held illegal. Before adopting that bill, I urge that you consider the reasons for allowing the program to continue.

Let's start with history, the life of any law. NSA's telephone metadata program cures a disastrous hole of our intelligence system, a hole exploited in the run-up to 9/11. Months before the attacks, NSA intercepted calls that one of the hijacking ringleaders, Khalid al Mihdhar, made between San Diego and 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. If NSA had known he was in the United States, he would have been caught long before September 11. But that crucial fact would not be discovered until a few weeks before the attacks. By allowing NSA's analysts monitoring foreign terrorists to see whether they have accomplices operating out of the United States, the metadata program closes a gap in our defenses – one that has already contributed to us losing three thousand lives.

But even so, you may ask, isn't it uniquely intrusive to allow the government to collect call records for all Americans, even those who are not suspected of any wrongdoing? Won't access to those records expose Americans to snooping on an unprecedented scale? In fact it will not.

As I've pointed out, billing records are not protected by the fourth amendment. That means they can be obtained by any government investigator with a subpoena.

And are they ever.

Law Enforcement Subpoenas Require Fewer Safeguards than NSA Follows

Today, law enforcement agencies collect 1.3 million telephone billing records a year using subpoena powers.[7] That means the average citizen is roughly a thousand times more likely to have his or her telephone calls reviewed by a law enforcement agency than by NSA. (And the chance that law enforcement will look at your records is itself low,

---

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").

[7] 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, and responses from, mobile carriers regarding use of cell phone tracking by law enforcement*, FORMER CONGRESSMAN (NOW SENATOR) ED MARKEY, http://www.markey.senate.gov/Markey_Letters_to_Wireless_Carriers.cfm, (last visited Nov. 20, 2013).

around 0.25% in the case of one carrier[8]). What's more, the billing records available to law enforcement agencies include the caller's name and other information, something that has been stripped from the NSA dataset. On top of that, there are no limitations on the kinds of searches that can be performed on subpoenaed billing records, on how long the records can be kept, or on how many investigators can review them. Finally, it is safe to say that every one of those subpoenas collects data that has little or nothing to do with investigation. For example the 8th Circuit upheld a grand jury subpoena to obtain every single transfer over $1000 that Western Union sent through a certain agent in Kansas City so that the government could search through the haystack for the needles of money laundering that were there.[9] Requiring investigators to show that every subpoenaed billing record is relevant to their case would cripple the investigation. Every subpoena is overbroad by that measure. And all of that has been true for as long as billing records have existed – nearly a century – without doing serious damage to our civil liberties.

In short, there's less difference between the NSA's "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 general relevance of its inquiry and is then allowed to collect and search the data more or less at will. 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. The standard in both cases is relevance and in both cases the government is limited to looking at documents relevant to its inquiry.

In fact, it turns out that NSA's access to telephone metadata for a critical counterterrorism purpose is far more constrained than the access routinely available to any big-city detective investigating a gambling ring.

Why "Collection First" Is Necessary

I recognize that gathering the data first and restricting the searches afterwards is unusual. It seems to put the cart before the horse. So why doesn't NSA perform its analysis the traditional way – by identifying the suspicious phone numbers and serving a subpoena for those numbers' contacts? Because in practice that will not work, at least not in time. 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 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.

---

[8] Letter from Timothy P. McKone, Exec. Vice President, AT&T, to then-Congressman Ed Markey, (May 29, 2012), http://www.markey.senate.gov/documents/2012-05-22_ATT_CarrierResponse.pdf (last visited Nov. 20, 2013).

[9] *See, e.g.*, *In re Grand Jury Proceedings*, 827 F.2d 301 (8th Cir. 1987) (permitting the subpoena and, *inter alia*, rejecting an argument that the subpoena should be quashed on grounds that it would make available "records involving hundreds of innocent people").

In response, some 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.

We are left with the stark reality that we must either use the collection-first model or risk a return to the days when the border marked a defensive seam that terrorists could exploit. 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.

The "USA FREEDOM Act" does not meet that burden. On the contrary, it kills the program without offering any plausible substitute. It is in every way a return to September 10, 2001.

2. The Role of the FISC and the Special Advocate

Before concluding my testimony, I would like to address one other issue in the USA FREEDOM Act. It concerns the FISC. Quite separate from its dismantling of the NSA's metadata program, the bill proposes to increase greatly the role of the court in overseeing domestic intelligence programs. For example, it appears to leave the FISC in charge of shaping, overseeing, and enforcing minimization guidelines in connection with section 215, pen/trap orders, and section 702, largely taking the Attorney General out of the process of writing minimization guidelines.

The FIS Court and 9/11

In so doing, the bill ignores history. The FIS court has taken control of minimization before, with disastrous consequences. The story was hidden for years by classified information rules, but it is well known now.[10] And it strongly counsels against giving the FIS court a larger role in overseeing minimization.

In the waning days of the Clinton Administration, stung by criticism that it was merely a "rubber stamp," the FIS court abruptly did by fiat what the USA FREEDOM Act would do legislatively. It took over the Attorney General's role by minimization requirements into its orders. It then used the minimization rules to build a "wall" between law enforcement and intelligence. By early 2001, it was enforcing that wall with unprecedented fervor, harshly disciplining an FBI supervisor who had not strictly observed the wall. The court had demanded an investigation that seemed to put the well-regarded agent at risk of a perjury prosecution. The court's message was clear: the wall must be observed at all costs.

[10] STEWART BAKER, SKATING ON STILTS 66-69 (2010).

Those costs would prove high indeed. Because in August of 2001, the FBI's premier counterterrorism task force found out that al Qaeda had sent two dangerous operatives to the United States. And it did … nothing. It did not use its elite team of agents or its extensive resource to track the two al Qaeda operatives. Instead, it was told to stand down; it could not go looking for the al Qaeda operatives because it was on the wrong side of the court's wall. Had it mobilized, the FBI task force stood a good chance of finding the hijackers – who after all were not hiding. The FIS court's bad legal judgment thus contributed heavily to the failures that led to 9/11. FIS court's minimization rules were thrown out on appeal, but not until after the attacks.

The FIS Court Since 9/11

That the court made terrible errors in 2001 is perhaps understandable. Repeating those errors is not. But the more closely I observe the FIS court the more concerned I become that the peculiar role that we have created for the FIS court makes a repetition all too likely.

The FIS court's principal statutory role is to approve or deny intercept and discovery orders involving foreign intelligence. This sounds like a role any court might play; judges approve warrants and wiretaps every day in a criminal context. In practice the FIS court's role is quite different. Sitting on the court involves judges in some of the most sensitive intelligence programs the United States has. It also exposes them to some of the most sustained and unidirectional political criticism they are likely to experience in their careers on the bench.

The court is routinely mocked as nothing but a rubber stamp, and it's clear that the mockery stings. In fact, the court recently announced that it was keeping statistics to show how often it forces modifications of FISA orders.[11] This suggests that the political criticism is hitting home, and perhaps affecting the court's ability to apply the law with an even hand. After all, no one would want to be judged by a court that goes out of its way to publicize a scorecard of how often it rules against him.

Why the FIS Court Is So Tempted to Overstep Judicial Bounds

In fact, though, the problem lies deeper. The FIS judges' sustained, high-tension exposure to the work of the intelligence agencies leads them to develop an overseer's mentality toward those agencies. As the court's "scorecard" and its occasional public statements suggest, the court feels obliged and entitled to flyspeck FISA orders, suggesting many modifications that may or may not be required by a strict reading of the FISA statute. Ordinarily, of course, if a judge asks the government for things that go beyond his authority, the government may appeal. But in the close confines of the FIS court, this is not an easy option. Neither the Justice Department nor the intelligence

[11] *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 (last visited Nov. 20, 2013).

community wants to alienate the FIS court by suggesting that its demands have no basis in law. Instead, it is more comfortable for all if the intelligence community adopts as many of the court's suggestions as it can. And so the FIS court stops being a judicial process of argument and ruling; it becomes more of a negotiation, in which the government is tempted to accept whatever the court asks for, whether justified by law or not.

Once the court has negotiated minimization guidelines, it owns them. The FIS court necessarily feels responsible for ensuring that they are carried out as intended. To make sure that happens, the court plays an increasingly managerial role in the operation of intelligence agencies.

But the FIS court is not a manager. Real managers 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 that its favored measures are required by law is very great. Similarly, when the court is disappointed or surprised by how the agency has implemented its measures, the temptation to reach for the contempt power is strong.

In short, the disaster of 2001 was not the result of one judge's bad temperament or faulty legal judgment. It is an institutional temptation, inherent in the managerial role that the FIS court has gradually assumed.

The USA FREEDOM Bill Will Encourage the FIS Court to Take Executive Responsibilities

The USA FREEDOM Act would exacerbate this dangerous trend. The statutory definition of minimization sets few limits on the court's discretion in overseeing the intelligence community. Any measure that is "reasonably designed" to "minimize" the impact on personal privacy can be squared with the statutory text, giving the court a standing invitation to engage in even more fine-tuned regulation of intelligence collection. But as the 2001 disaster surely shows, giving a large managerial role to the FIS court probably violates the constitutional separation of powers and certainly violates common sense.

The Special Advocate Provisions

The bill's title creating a special advocate compounds this error. A special advocate is almost certainly unnecessary. 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. The staff attorneys 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.

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? Do you argue for the greatest possible privacy protection even at the risk or serious intelligence failures or do you take account of the practical needs of the intelligence community? To take one example, the bill authorizes the special advocate to appeal any decision and requires the court of review to hear the appeal. Could the special advocate decide that the best way to "vigorously advocate … in support of legal interpretations that protect individual privacy and civil liberties" is to appeal every single FIS order, including extensions, forcing the government to let the interceptions lapse while the cases are processed on appeal? No lawyer with a real client, or a superior who answered to the President, would do so. But the special advocate has neither.

In questioning the wisdom of special prosecutors, Justice Scalia once described as frightening the prospect 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.[12] 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 years, just to be able to argue that U.S. intelligence programs are unreasonable, overreaching, and unconstitutional? To update the old saw, a lawyer who represents himself has an ideologue for a client.

The office of special advocate envisioned by the bill is, if anything, even more independent than Ken Starr or Lawrence Walsh ever was. Under section 902 of the bill, the special advocate, removable only for "good cause shown," is appointed by the Chief Justice, a judicial branch official, from a list supplied by an independent agency. This is likely a violation of separation of powers by itself, but other provisions are equally troublesome on that score. Among the constitutional questions raised by the bill are:

- Whether Congress may require that a member of the judicial branch like the special advocate meet a statutory litmus test such as a "demonstrated commitment … to civil liberties," as section 902 does?
- Whether Congress may confer appellate standing in a case on a lawyer by legislative fiat, as section 904 does?

[12] *Morrison v. Olson*, 487 U.S. 654 (1988) (Scalia, J., Dissenting).

- Whether Congress may give a quasi-governmental official roving authority to reopen and relitigate already decided cases, as section 903 provides?

Protecting national security is a solemn responsibility for the judges of the FIS court and the agencies that appear there; asking them to adjudicate a host of questionable constitutional experiments adds unnecessarily to their already heavy burden.

Even if the special advocate provision survives constitutional scrutiny, the office will surely become an extension of the court, answerable to the judges and eager to please them. But that outcome will simply foster the FIS court's constitutionally dubious relationship with the intelligence community, giving the court far greater resources to explore and tinker with intelligence management – without taking responsibility for the result. Under the bill, the special advocate can create a vast "advocacy" to support his or her office. The special advocate may "appoint and terminate and fix the compensation of employees" without regard for the competitive service – or any budgetary oversight, for that matter. The special advocate may also retain outside lawyers to supplement this staff. It's true that the staff and outside lawyers must get clearances, but the statute creates an affirmative obligation for the government to issue those clearances "expeditiously" and "to the extent possible under existing procedures and requirements." This invites the special advocate to question the security clearance process in a way that I have not seen before, allowing the special advocate to threaten lawsuits if the clearances are denied or come too slowly. Clearances granted under such pressure will be no more certain of catching problems than the clearances granted to Edward Snowden. The FIS court can also send the special advocate out as a kind of roaming inspector, ordering the intelligence community to give the advocate "any documents or material necessary" to carry out his duties. The special advocate may propose declassification of documents, and it appears that declassification decisions, an unprecedented change at least some classification decisions, previously reserved to the executive branch, will be left to the judiciary.

All of these provisions bring the FIS court even closer to being a kind of parallel government, managing vital executive functions from the judicial branch. Many of us saw the damage that such a confusion of roles could do in August of 2001, and we will never call the judiciary the "least dangerous branch" again.

Conclusion

I've focused my testimony on the most serious issues raised by the USA FREEDOM Act. The telephone metadata program operated under section 215 should be retained, not abolished. The FIS court should be carefully confined to a judicial role. Any changes to FISA that extend the court's reach further into executive functions, including the creation of a formal "special advocate" before the court, should be rejected.

There are many other issues that this committee might wish to examine. One issue in particular is the remarkable hypocrisy of European and other countries' attacks on US

intelligence and surveillance standards. A as I testified before this Committee[13] in July and before the House Permanent Select Committee on Intelligence last month , [14] the standards for privacy protection are far weaker in Europe and elsewhere. I'd be glad to discuss the international issues and possible ways to protect U.S. companies during the hearing.

[13] Testimony of Stewart A. Baker, Oversight Hearing on FISA Surveillance Programs, United States Senate, Committee on the Judiciary (July 31, 2013) *available at* http://www.judiciary.senate.gov/pdf/7-31-13BakerTestimony.pdf.

[14] Testimony of Stewart A. Baker, Hearing on Potential Amendments to the Foreign Intelligence Surveillance Act, U.S. House of Represenatives, Permanent Select Committee on Intelligence (Oct. 29, 2013), *available at* http://intelligence.house.gov/sites/intelligence.house.gov/files/documents/Baker10292013.pdf.