Before the United States Senate Select Committee on Intelligence

The Senate of the United States

On the USA FREEDOM Act (H.R. 3361 / S. 1599)

June 5, 2014

Testimony of Stewart A. Baker

Partner, Steptoe & Johnson, LLP

Chairman Feinstein, Ranking Member Chambliss, members of the committee, it is an honor to testify before you today on the USA FREEDOM Act. I have a longstanding interest in the topics today's hearing will cover. I served as the General Counsel of the National Security Agency from 1992 to 1994, under Presidents George H.W. Bush and Bill Clinton. I was General Counsel of the Silberman-Robb Commission that investigated intelligence failures on weapons of mass destruction in Iraq and elsewhere. From 2005 to 2009 I served as Assistant Secretary for Policy at the Department of Homeland Security. I have also worked and commented on national security and intelligence issues while a private attorney.

I testify before this distinguished committee today in order to offer my view that the USA FREEDOM Act, if passed as currently drafted, will be a memorable wrong turn for the United States and for the cause of intelligence under law. The decision to outlaw domestic collection and storage of data undercuts our intelligence agencies' ability to use the best technology to protect the nation. It substitutes wishful thinking and faux outrage for the hard work of devising privacy protections that will work in the twenty-first century. We will regret it.

Even more regrettable are the efforts to make the bill worse, to turn the bill into a strait-jacket from which our intelligence agencies cannot possibly escape. The critics of the House bill want guarantees that our intelligence agencies can never do anything Congress has not foreseen and approved in detail. But those who advocate such limits have no crystal ball. They do not know what future threats we will face. They do not know what clues we will need to thwart those threats. Yet they presume to tell our intelligence agencies which clues they may pursue and to foreclose all others, now and forever. To call theirs a foolish pride is almost too kind.

The End of Bulk Collection

The USA FREEDOM Act as it stands will make Americans less safe while contributing little or nothing to their privacy. The bulk collection program the bill abolishes grew from a very real intelligence failure. In the run-up to 9/11, NSA intercepted calls to Yemen from a terrorist in San Diego, but in a costly deference to the civil liberties concerns of the 1990s, NSA had never developed a way to track calls back to the United States.[1] The metadata program closed that gap.

[1] I'm aware that civil libertarians have worked overtime to contradict this statement. But it is a matter of simple fact that NSA was not able to identify these calls as coming from San Diego. The critics end up making a very different claim. They say that NSA knew in general terms about the San Diego

This bill will open it again. Under its strictures, if NSA identifies a suspect foreign number, it will no longer be able to do a quick and reliable database search to find out who is calling the number from this country. Instead, it will have to ask a dozen carriers to hand over whatever information they may have on that number – data they may store in very different formats and for different historical periods. There will be fewer dots, and connecting them will be harder.

The threat that this program was designed to counter is the most dangerous one we face – a well-organized cross-border terrorist attack. The most dangerous terrorist groups have foreign havens where they can plan and recruit and train far from the country they intend to strike. That threat is as real as today's headlines. Today, there are al Qaeda offshoots and clones operating freely in Syria, in Libya, in Sub-Saharan Africa, in Yemen, and in Pakistan. If they can get the breathing space, they will train a new generation of terrorists to kill Americans in large numbers here at home.

The 9/11 hijackings may have been the first but they were not the last such large-scale cross-border terror strike. The 2008 Mumbai attackers trained in Pakistan for months, then a few were hand-picked for the mission.[2] They used every advantage of modern technology – GPS navigation, Google maps, VOIP handsets and satellite phones.[3] A team of handlers in Pakistan talked the killers through the city from what appears to have been a 24-hour terrorist operations center, providing tactical guidance and relaying information from live news coverage of the event.[4] The attacks convulsed Mumbai for days, killing over 150 people.[5]

It's worth examining how an attack like Mumbai's would be handled before and after the USA FREEDOM Act. Until recently, if terrorists in the United States were coordinating by phone with a foreign operations center, NSA would enter the phone numbers of the operations center

---

terrorist or that it should have known he was coming to the United States or that it would have known if the CIA had done a better job of sharing information. Even if these statements are all true, the fact remains that NSA, as a signals intelligence enterprise, had no efficient way to identify calls coming from the United States to suspicious numbers abroad. A few critics say that the NSA should have been able to determine the calling as well as the called number. In fact, that might be true for Yemeni police conducting a standard wiretap; it is not reliably true for other forms of intercept. And again, this claim falls before one simple fact: NSA was not able to identify the location of the caller.

[2] Somini Sengupta, "At Least 100 Dead in India Terror Attacks," The New York Times, November 26, 2008, http://www.nytimes.com/2008/11/27/world/asia/27mumbai.html?pagewanted=all.

[3] Emily Wax, "Mumbai Attackers Made Sophisticated Use of Technology," The Washington Post, December 3, 2008, http://www.washingtonpost.com/wp-dyn/content/article/2008/12/02/AR2008120203519.html; Rina Chandran, "Mumbai attacks show up India's technology shortcomings," Reuters, December 11, 2008, http://www.reuters.com/article/2008/12/11/india-mumbai-tech-idUSBOM33944720081211.

[4] Rina Chandran, "Mumbai attacks show up India's technology shortcomings," Reuters, December 11, 2008, http://www.reuters.com/article/2008/12/11/india-mumbai-tech-idUSBOM33944720081211.

[5] "At Least 150 Dead in Mumbai Attacks," PBS NewsHour, November 28, 2008, http://www.reuters.com/article/2008/12/11/india-mumbai-tech-idUSBOM33944720081211.

into its database and immediately know all the U.S. numbers that were in touch with the center, as well as anyone else in the country who had been in contact with the terrorists. If the attackers switched SIM cards (and thus phone numbers), the new numbers could be added to the search immediately.

Under USA FREEDOM, however, NSA could not search for calls from the United States to the foreign operations center until it had satisfied the Foreign Intelligence Surveillance Court (FISC) that it had a reasonable and articulable suspicion about the center. Or it could persuade the Attorney General that it has such a suspicion and that conducting the search was an emergency. That could be done, but it would be more likely to take hours than minutes. Then the search would go to a host of phone carriers in the United States, some of whom might be able to respond electronically while others respond only by exchanging paper. The searches themselves would depend on the varying information systems of each carrier. If the attackers chose small and obscure carriers for their phone service, this might be the first 215 metadata request sent to the carrier. Again, the responses would trickle in over a period of many hours – if we were lucky. If the attack occurs on a long weekend, it could take as much as a day to track down the carrier employees who need to respond. And updating the data as the attackers swap SIM cards would mean repeating the process at each carrier for every change the attackers make. Hours of delay are a near certainty at a time when every few minutes brings another death.

As Mumbai shows, modern technology often empowers terrorists. If we deny new technology to our intelligence agencies, we face a steady worsening in our ability to respond to attacks. Yet at bottom, the USA FREEDOM Act is an effort to reject new technology. The fact is that data is getting cheaper to collect, to store, and to analyze. This new technology is one of the most promising tools we have to find and thwart terrorists. The USA FREEDOM Act denies this tool to our intelligence agencies. And for what? Ending NSA's program will not end bulk collection of data in the private sector or by government agencies using other authorities, here and abroad.

In fact, law enforcement agencies have routinely collected telephone metadata for close to a hundred years. In recent years, they have served more than one million subpoenas a year for such data.[6] In contrast, NSA never provided the FBI with more than 500 numbers in a year, under heavy judicial and congressional supervision.[7] The bill will make those 500 searches much harder and much less effective but it won't measurably change the government's overall access to metadata.

This bill is privacy theater, and dangerous theater at that.

We would be safer, and so would our privacy, if instead of launching a hopeless campaign to limit front-end collection of data, Congress focused on restricting and auditing access to the data once collected.

---

[6] Eric Lichtblau, "Wireless Firms are Flooded by Requests to Aid Surveillance, The New York Times, July 8, 2012, http://www.nytimes.com/2012/07/09/us/cell-carriers-see-uptick-in-requests-to-aid-surveillance.html?pagewanted=all&_r=0.

[7] Ken Dilanian, "Concerns about NSA surveillance persist despite release of files, Los Angeles Times, July 31, 2013, http://articles.latimes.com/print/2013/jul/31/nation/la-na-nsa-surveillance-20130801.

Worse, by passing this bill, Congress will guarantee a decade of risk aversion in the intelligence community.

Some will say that's what they want, an intelligence community that is averse to activity that might affect the civil liberties of Americans.

That sounds noble, but it's going to get people killed.

After all, the notorious wall between law enforcement and intelligence was also put in place to keep the intelligence community from affecting the civil liberties of Americans. And it was to protect civil liberties from a hint of intelligence influence that the Foreign Intelligence Surveillance Court drove the wall deep into the FBI in 2001 – without any basis in law.[8] Unexamined appeals for "more" civil liberties protection are what paved the road to 9/11, and they will pave the way again if this bill passes.

We cannot afford an intelligence community that is afraid to collect intelligence on our enemies, but that will be the legacy of the USA FREEDOM Act.

USA FREEDOM Act and Specific Selection Term

Now let me turn to the astonishing effort to make the bill worse than it already is.

The most egregious of those efforts concerns the bill's provision requiring that all section 215 requests contain "specific selection terms." Everyone recognizes that if bulk collection requests are foreclosed, then the government must make individualized requests for data. And to do that, it has to give the companies specific search terms to use. Before amendment, the House bill said that the government could only ask the companies to use three kinds of search terms. They could only ask the companies to look for a suspicious "person, entity, or account."

This was foolish. Clues come in many forms. What if the agency doesn't know the suspect's name but does know his internet address, or the unique identifier of his tablet? Those are proper and specific search terms, and they are likely to be of value to terrorism investigators. So the bill was revised; now it allows the agency use search terms "such as … a person, entity, account, address or device."

Some opponents have a beef with the addition of "address or device." They claim that these words are too open-ended and ambiguous. But when asked to identify the ambiguity they fear, the critics offer only strained and unlikely interpretations. Senator Ron Wyden has said that the law as adopted by the House "could be used to collect all of the phone records in a particular area code, or all of the credit card records from a particular state."[9] This apparently rests on the remarkable view that a state or an area code is the same as an "address." Wow. I knew Oregon was a big state, but I'm still surprised to hear that they're using area codes as addresses out

[8] Stewart Baker, "The Wall and the Least Dangerous Branch," The Volokh Conspiracy, June 14, 2010, http://www.volokh.com/2010/06/14/the-wall-and-the-least-dangerous-branch/.

[9] "Wyden Opposes Watered-Down USA Freedom Act," Office of Senator Wyden Press Statement, May 22, 2014, available at http://www.wyden.senate.gov/news/press-releases/wyden-opposes-watered-down-house-usa-freedom-act.

there.[10] Let's be realistic. If that can be called an ambiguity, then no words will ever satisfy the critics. Why not object to the word "person," for there are cases treating entire cities or counties as persons?[11]

And dropping those words from the bill create obvious and dangerous gaps in our ability to investigate terrorism. Take these examples:

- Suppose that attackers use a VOIP phone as in Mumbai. The phone might have only an IP address. If we drop "address" from the list, the government can't serve a 215 order asking for information about the online activities of that phone.

- Or suppose that in a Mumbai-style attack the terrorists keep changing their SIM cards (and thus phone number); we would need to search not for the phone number but for the IMEI number that identifies the actual phone. Drop "device" from the list and the government can't ask for that information.

Other opponents aim their fire at the words "such as." They would drop those words, capping the list of search terms at five, or even three. This too is foolish and dangerous. Can the proponents of this change predict with perfect foresight which clues we'll need to uncover the next conspiracy? I doubt it.

Again, a few examples show why we cannot foreclose the use of other specific search terms:

- What if we pick up intelligence that tells us that a terrorist is staying in a particular hotel room and we want the hotel to produce his name? Is a hotel room an address? Without "such as" in the list, we'll still be in court arguing about that when he checks out.

- What if we face a terror attack like the Washington sniper case? Can we use section 215 to ask the phone companies to give us the numbers of any phones that were active in the vicinity of all five shootings when they occurred? That's plenty specific, and a good idea too. I fear that even the current language might make it impossible for counterterrorism investigators to make such a request.

- What if we learn a terror suspect's license plate number? Can we use section 215 to search DMV records for his name? Not if we're limited to the five terms listed in the statute.

I suppose that the practical answer to some of these questions is that the government won't use its counterterrorism or national security authorities. It will rely on criminal subpoenas, which

[10] There is not much law on this, but courts have held that a zip code is not an "address." *Hancock v. Urban Outiftters, Inc.*, 2014 WL 988971 (holding that a zip code is not the same as an address, as defined in the District of Columbia Consumer Identification Information Act and the District of Columbia Consumer Protection Procedures Act).

[11] *See Monell v. New York City Dep't. of Social Services*, 436 U.S. 658, 659 (1978) (declaring that a particular claim could be brought because Congress intended municipalities and local governments to be persons under the relevant provision).

don't come with any of these restrictions. But if that is so, if the intent is to let our intelligence agencies have all this information as long as they rely on law enforcement authorities, then we're back to privacy theater. Or privacy farce, since the result of the legislative changes is to put the United States Congress on record as giving fewer tools to those investigating terrorism and national security threats than to those pursuing muggers and embezzlers.

The Public Advocate

The act also "[r]equires the FISA court and the FISA court of review to appoint an individual to serve as *amicus curiae* to assist in the consideration of any application for an order or a review that presents a novel or significant interpretation of the law, unless the court issues a finding that such appointment is not appropriate."[12]

This provision is plainly better than the elaborately staffed and entitled "advocracies" that other proposals would create. But it is still fraught with problems. Let me touch on two.

First, the bill calls for the identification of five lawyers who will be available to file as amicus curiae. On one level, this makes sense, because they'll need to be cleared in advance, and they'll need deep familiarity with the law. But where will these lawyers come from? If they come from private practice or a trade association or nonprofit advocacy group, will their positions as amicus be influenced by the interests of their clients or employers or donors, who may well include many foreign nationals, corporations, or governments? There is a serious risk of subtle or not-so-subtle influence, unless the advocates-in-waiting consist of retired lawyers and judges without clients. At a minimum, the law should set the strictest ethical standards to avoid even a hint of conflict of interest.

Second, in my experience, the whole idea of routinely appointing special advocates suffers from a misconception that the current system consists of an aggressive advocate and an empty chair in front of a judge. In fact, the government rarely goes all out for a maximalist position in the FISC. It regularly pulls its punches; because the hearings are usually ex parte, the Justice Department has a long tradition of trying to be as much a referee as an advocate. The NSA is not even allowed to appear and argue on its own behalf in the FISC.

Let me be blunt. If we want an adversary presentation in front of the FISC, then we need two sides arguing strongly for their positions, not an aggressive amicus and a referee. Someone should present the argument in favor of gathering the intelligence we need to stop terrorists and foreign spies. At a minimum, I suggest that, any time the courts invite an amicus to make the case for greater privacy, they should also invite NSA to make its case to the court as well, unfiltered by the Department of Justice.

[12] USA FREEDOM Act, H.R. 3361, 113th Congress (2013-2014), available at http://beta.congress.gov/bill/113th-congress/house-bill/3361.