

Statement for the Record

Senate Select Committee on Intelligence

"A Shield and a Sword: Reforming the Foreign Intelligence Surveillance Act"

Timothy H. Edgar

**Visiting Fellow, Watson Institute for International Studies
Brown University**

September 26, 2013

Chairman Feinstein, Vice Chairman Chambliss, and Members of the Committee, thank you for this opportunity to testify at this rare public hearing to consider reforms of the Foreign Intelligence Surveillance Act (FISA).

My testimony will put proposed reforms into context by examining whether they enhance values of *transparency, accountability, and privacy*, and whether they do so consistent with the government's compelling need to collect vital intelligence to keep the country safe.

Privacy, Inside and Out

My perspective on these issues is shaped by my unique experience as a privacy and civil liberties lawyer both inside and outside the government.

In the immediate aftermath of the September 11 attacks (from 2001 through 2006), I was the national security legislative counsel for the American Civil Liberties Union (ACLU). I spearheaded the ACLU's advocacy in Congress on issues such as the USA PATRIOT Act and intelligence reform.

During the second half of the Bush Administration, I had an unusual opportunity to go inside the surveillance world. From 2006 to 2009, I became the Deputy for Civil Liberties in the newly-created Office of the Director of National Intelligence (ODNI), with oversight of sensitive intelligence programs, including the now-declassified programs we are discussing today. It was not an easy decision, given the tensions between the civil liberties community and the Bush Administration.

From 2009 to 2010, I served as the first ever Director of Privacy and Civil Liberties on the White House National Security Staff, with a focus on cybersecurity issues. This position fulfilled a commitment made by President Obama in his remarks on cybersecurity to designate "an official with a portfolio specifically dedicated to safeguarding the privacy and civil liberties of the American people."¹ From 2010 to 2012, I returned to the ODNI to serve in the Office of General Counsel.

Today I am a visiting fellow at Brown University's Watson Institute for International Studies, where I teach and write about privacy, cyber security and Internet freedom.

FISA: From Shield to Sword

The intelligence community is facing perhaps the most serious crisis in public confidence since the Church Committee era of the 1970's. Ordinary Americans no longer believe that the intelligence agencies can be trusted to respect their privacy and civil liberties. Edward Snowden's reckless dump of top secret documents, followed by his bizarre flight to those new champions of Internet freedom – China and Russia – should have turned Americans against him. Instead, a majority – across the political spectrum – regard him as a whistleblower, believing their fears of government snooping on a massive scale have been confirmed.²

These FISA collection programs are certainly, in words of Director of National Intelligence James Clapper, "broad in scope."³ FISA business records orders, now declassified, require major telecommunications providers to provide "on an ongoing daily basis," metadata that relates to "*substantially all of the telephone calls* handled by the companies, including both calls made between the United States and a foreign country and calls made entirely within the United States."⁴

Collection and analysis of Internet communications content is also vast. In a recent public report, the National Security Agency says that it "touches" 29.21 petabytes of data every day.⁵ According to the same NSA report, this represents about 1.6% of total daily Internet traffic. By comparison, Google analyzes a smaller, although still quite vast, 20 petabytes per day.⁶ While the NSA's collection is directed at foreign targets and only a small fraction (0.025% of the 29.21 petabytes, or 0.00004% of all Internet traffic) is actually selected for review – this is Internet surveillance on a very impressive scale.

Much of this collection is both enabled and regulated by the amendments made to FISA after the September 11, 2001 attacks in sections 501 and 702. These new authorities, and the manner in which the government has employed them, represent a major transformation of FISA – from a shield that protects American civil liberties, to a sword authorizing major collection programs.

Prior to 9/11, FISA authorized a relatively narrow range of intelligence activities, mainly by providing judicial review of national security wiretaps under Title I of FISA and searches under Title III of FISA. Such wiretaps and searches had previously been conducted by the Executive Branch acting alone, with disastrous results for civil liberties. The enactment of FISA in 1978 was in large part a reaction to abuses of those intelligence powers, as documented by the Church Committee.

Today, FISA authorizes vast intelligence collection programs involving telephony metadata and Internet communications. These programs make aggressive use of

the broad authorities granted by Congress in the USA PATRIOT Act to compel production of business records and other “tangible things” (under section 501 of FISA, although sometimes called “section 215” authority),⁷ and in the FISA Amendments Act to compel broad acquisitions of communications content targeting foreign persons located outside the United States (under section 702 of FISA).

To be clear, the collection enabled by these new authorities is vital. As this committee well knows, surveillance gaps prior to 9/11 made it impossible for the NSA to connect a telephone call originating in Yemen to Khalid al-Mihdhar, a 9/11 hijacker then in San Diego. While the NSA had the terrorist number in Yemen under surveillance, it did not have the data from the domestic side of the call and therefore did not know that the hijacker was inside the United States.⁸

The new FISA authorities close this and other gaps, and do so without the dangers of executive unilateralism of NSA surveillance outside of FISA during the first half of the Bush Administration. Intelligence officials have testified that the new authorities have aided in the prevention of 54 international terrorist attacks worldwide – including 13 attacks targeting the United States homeland.

The “business records” provision of FISA was important in preventing 12 of these homeland attacks.⁹ Section 702, allowing the targeting of foreign persons outside the United States, has also proved instrumental in disrupting plots in the United States. For example, section 702 surveillance aided in the disruption of a plot to bomb New York City subways. In 2009, federal authorities were able to use intelligence information obtained under section 702 to track Najibullah Zazi to New York City and disrupt his plans before he could plant a bomb.¹⁰

Nevertheless, the fact that intelligence collection is necessary – even vital – does not end the inquiry. In an era of “big data,” these broad new collection authorities raise serious, and novel, privacy and civil liberties problems.

Reforming the Foreign Intelligence Surveillance Act (FISA)

This committee is not new to the challenge of crafting laws that enable the world’s oldest constitutional democracy to run the world’s most powerful intelligence apparatus. The Foreign Intelligence Surveillance Act (FISA) represents a major achievement in that endeavor, putting national security surveillance on a sound legal basis. It is a unique law among democracies in that it puts a court, rather than a government official, in charge of approving intelligence surveillance orders.

The intelligence business has not always comfortably fit with American values of openness, democratic accountability, and respect for privacy. Proposals to amend FISA should make reforms that enhance these three fundamental values. First, FISA should become much more *transparent*. While many FISA activities will properly remain classified, the public should be aware of the broad scope of FISA activities and the major interpretations of the Foreign Intelligence Surveillance Court (FISC or

FISA Court). Second, the FISA system must be made more *accountable to the democratic rule of law*. Principally, this will involve strengthening the FISA court system to make it more like other judicial bodies. Finally, FISA collection authorities and safeguards should, over time, be modified to require new protections for *privacy and civil liberties*. This will require the development of alternatives, using innovative privacy enhancing technology, to the current system of very broad collection (for example, of call detail records), coupled with back-end protections.

Enhancing Transparency

The public and the government see intelligence surveillance under FISA through very different prisms. Those on the inside see carefully crafted programs governed by a complex body of guidelines that protect privacy – administered by an army of lawyers, scrutinized by Congress, and subject to review by the Foreign Intelligence Surveillance Court (FISC).

Those on the inside sometimes forget that the public sees none of this. Instead, the public perceives a disturbing pattern of secret government and secret law, accompanied by government assurances to “trust us, we are keeping you safe.” There are real and meaningful privacy and civil liberties safeguards in FISA collection, yet the way these safeguards operate has been – until now – as highly classified as the programs themselves.

For decades, the only information released to the public concerning FISA surveillance was the number of applicants sought and the number granted – very often, the same number, leading to the misimpression that the FISA court was a rubber stamp. (In reality, applications were often withdrawn, modified, or negotiated before ever being officially submitted to the court.) Perhaps reporting applications sought and granted made sense when the court mainly reviewed individual surveillance and search orders – these numbers were potentially useful in understanding the scale of FISA surveillance. Today, these numbers are woefully inadequate.

The Director of National Intelligence (DNI) has determined that significantly more information can be released, including a breakdown of the number of orders under particular FISA authorities – individual surveillance and search orders, orders for business records or other “tangible things,” FISA Amendments Act orders under section 702, pen register/trap and trace orders, and national security letters (which are not FISA authorities but are intelligence authorities). More importantly, this public breakdown will also include not just the number of orders, but the number of *targets* affected by such orders.¹¹

This increased transparency is welcome, and should go further. For example, S. 1452, the Surveillance Transparency Act of 2013, would also require reporting of at least a good faith estimate of the number of United States persons whose

communications or records are collected, and the number whose information is actually examined.

Such proposals will need to balance transparency with the need to protect sources and methods. It goes without saying that information that could reveal particular targets of surveillance should never be revealed. Likewise, the government should not provide a list of which companies are participating in surveillance programs. While the participation of major companies will not be hard to surmise, there should be some uncertainty. If terrorists or other foreign targets know with certainty which providers are *not* providing information to the government, they will know which ones to use.

Rather than providing a list of companies, the government should detail the major categories of data that are being obtained that include United States person information. For example, the American public now knows that its call detail records are obtained by the FISA court, under particular safeguards. The public should also know what other uses are being made of the business records and “tangible things” authority under the FISA court’s very broad interpretation of that power, and pursuant to what safeguards.

Ensuring Accountability

The Foreign Intelligence Surveillance Court (FISC) and the Foreign Intelligence Surveillance Court of Review (Court of Review) are very unusual judicial bodies. The public expects that courts generally operate in the open, hear from both sides, and that judges are selected in a manner that fosters democratic accountability while ensuring judicial independence. The FISC and the Court of Review suffer a deficit in these areas – a deficit that can be corrected.

Operating more in the open. First, the FISA court’s opinions and orders interpreting the law or addressing constitutional issues should be public as a matter of course, with appropriate redactions to protect national security. This would enhance transparency, of course, but it would also strengthen the credibility of the FISA court in the eyes of the public, making it more like a normal court.

The excessive secrecy of the FISA court process has engendered mistrust and distorted national debate on at least three separate occasions. We know of these only because of the release of previously classified FISA court opinions:

- First, the FISA court’s very broad interpretation of what business records or other “tangible things” are “relevant” to an authorized investigation of international terrorism is what permits the NSA call detail records program.¹² While relevance is a broad legal concept, the idea that *all* of the data in a massive database is “relevant” – even in the context of a program with meaningful back-end safeguards to narrow the information, once collected – is a novel one. Those who were not aware of this interpretation –

including key members of Congress who did not take advantage of classified briefings, as well as many knowledgeable lawyers and national security experts – can be forgiven for their surprise and even dismay that this provision of the Patriot Act was used in this way. Certainly, the issue was never seriously debated during two reauthorizations of the Patriot Act.

- Second, the NSA's interpretation of the requirement in section 702 that acquisitions of communications (including Internet communications content) must include procedures that "target" foreign persons outside the United States is similarly surprising to those on the outside.¹³ The FISA court's recently released opinions show that communications that "target" foreign persons include not only communications that are "to" or "from" that person, but also those that are merely "about" that person (in that a particular selector, such as an e-mail address, appears in that communication). Moreover, even communications which are not to, from or about the foreign target at all have been acquired as a result of the manner in which some collection was conducted by the NSA. Misunderstandings about this resulted in the FISA court finding that the NSA had violated the Fourth Amendment for three years, and tightening minimization procedures for this type of collection.
- Finally, the FISA court's pre-9/11 concerns about the sharing of FISA surveillance with criminal investigators and prosecutors – and the resulting "wall" that contributed to the failure to prevent the 9/11 attacks – is a similar example of where the excessive secrecy surrounding FISA court opinions distorted public debate.¹⁴ There was little public awareness, and no public pressure, to correct this information sharing problem before the 9/11 attacks. A more open FISA court process might have highlighted the issue in a way that encouraged Congress to address this issue earlier.

As the last example illustrates, transparency about the FISA court's interpretation of the law is important not only for a robust debate about privacy and civil liberties. It is also important in ensuring that these authorities remain robust and effective in protecting national security.

Hearing more than one side. Second, the FISA statute should be amended to provide a mechanism for the court to hear arguments to protect civil liberties and privacy. One example of how to do this is S. 1467, the FISA Court Reform Act of 2013. S. 1467 creates a special advocate to "protect individual rights by vigorously advocating before the FISA Court or the FISA Court of Review, as appropriate, in support of legal interpretations that minimize the scope of surveillance and the extent of data collection and retention."

This would be a major shift from the current process, which is ex parte unless a data provider (not an ordinary citizen) objects. Of course, an ex parte process is not

necessarily an illegitimate process. Ordinary courts, when hearing applications for wiretap orders and search warrants, generally hear only from the government side. However, the FISC and the Court of Review are not ordinary courts. They grant surveillance and search orders that are likely never to result in evidence which will be presented in a court and subject to challenge. Under the new, broader authorities granted after 9/11, they oversee complex and vast intelligence collection programs with major impacts on privacy and civil liberties.

One need only read the most recently declassified FISC opinions to wonder how they might have been different if the judges had heard from another side. Of course, care must be taken to ensure that more subtle pressures also do not influence the advocate's work. A lawyer who is hoping for a long and fruitful career in national security law may be concerned about winning arguments against government surveillance powers a bit too often. A weak or timid special advocate would be worse than the current ex parte system, where at least the judges know that they are only hearing one side.

Perhaps even more useful than a special advocate would be a special master or team of special masters, trained in computer science, to assist the court in understanding the complex nature of NSA surveillance. Many of the most serious compliance problems faced by the FISA court have resulted from basic misunderstandings about how the surveillance itself works. If a government official, special advocate, and judge – lawyers all – lack real technical expertise, serious problems will continue to persist for years based on simple misunderstanding, even with vigorous advocacy on both sides.

Selecting judges. Finally, Congress should reform the way in which judges to the FISC and the Court of Review are selected. FISA gives this power exclusively to the Chief Justice of the United States. As a result, there has always been a danger that the judges would reflect the ideology of the Chief Justice and would be skewed as a result.

Prior to 9/11, this problem remained largely theoretical. The FISC was generally a well-balanced body. Chief Justices Burger and Rehnquist, while sympathetic to surveillance arguments, generally appointed a FISC with a well-balanced membership. The Court of Review was unimportant as it had never even met. Today, this problem has become significant. Chief Justice Roberts has stacked the FISC with judges who are sympathetic to the government's side.¹⁵ The Court of Review likewise skews toward the government side, and its opinions are becoming more frequent and far more important.

One way to ensure a more balanced FISC and Court of Review would be to enact S. 1460, the FISA Judge Selection Reform Act. The bill would keep the selection of the FISC and Court of Review within the judiciary, but would broaden the selection process. The Chief Justice would select thirteen FISA court judges from among no more than three names submitted by chief judges of each of the judicial circuits. The

Court of Review judges would be named by the Chief Justice only with concurrence of five associate justices.

Protecting Privacy

Finally, Congress should consider, over time, requiring the new FISA authorities to provide greater protections for privacy through innovative, privacy-enhancing technology. Even with robust and meaningful back-end privacy safeguards, the NSA call detail records program should give any thinking person pause. NSA collection of "*substantially all*" of the call detail records of major companies – including domestic calls – is at best suboptimal, and at worst a privacy disaster waiting to happen.

Even without any malicious intent, the scale of the program has already resulted in significant compliance problems, resulting in the FISC essentially taking over for several months the process of selecting "seed" numbers that permit individual analysts to review call detail records.¹⁶ Similarly serious problems resulted from misunderstandings about how Internet communications were collected under section 702 of FISA. It is very unlikely that these program can continue indefinitely without additional compliance incidents, or even abuse, especially as the intense public scrutiny fades.

The biggest danger may not be political misuse of the NSA's data by a future Richard Nixon or a future J. Edgar Hoover, but the threat posed by having such sensitive data amassed in a large government bureaucracy that has not shown itself capable of keeping data secret. While the safeguards are tight, nothing is foolproof. A future Snowden might sell access to the NSA's surveillance apparatus to our adversaries. Are we so confident he or she would be caught? As long as massive collection continues, the danger persists.

The answer lies not in repealing the new authorities, but in phasing in requirements to use innovative, privacy-enhancing technology to access data without amassing it in bulk. The Office of the Director of National Intelligence has for years sponsored research into sophisticated, privacy-enhancing cryptographic techniques that could allow the NSA to have access to the information it needs – and only the information it needs – while providing sound privacy assurances.¹⁷

These research programs have developed secure distributed private information retrieval (PIR) protocols that permit an entity (such as the NSA) to query a cooperating data provider (such as a telecommunications provider) and retrieve only the records that match the query without the data provider learning what query was posed or what results were obtained. This technique would greatly aid more targeted data acquisitions by minimizing the danger to national security of revealing the government's interest in particular data – a danger that is a major reason the NSA may prefer bulk collection over individualized queries.

Such techniques may not be reassuring if there are no guarantees the queries are appropriate. The research has also examined how to automatically ensure that complex queries are in accordance with privacy policies. Research continues into more complex queries of dynamic databases and more robust assurance to both the intelligence agency and the data provider of compliance with privacy policies. In the future, privacy protection may use very advanced cryptographic techniques such as fully homomorphic encryption – a technique that allows computations on encrypted databases, producing a valid encrypted result that nevertheless maintains the privacy of the database.

Practical deployment of such technologies could provide a breakthrough that would represent a real alternative to the massive collection the NSA now undertakes. Congress needs to spur the intelligence community along. As long as the government views these technologies as optional, deployment will lag. The Congress could phase in mandates for deployment of privacy-enhancing technology with sunsets for the broader collection authorities which these technologies would make obsolete.

Conclusion

Meeting the national security threats of the 21st Century – international terrorism, cyber insecurity, proliferation of weapons of mass destruction, weak and failing states – requires robust and powerful intelligence capabilities. The weaknesses in the pre-9/11 FISA regime were amply documented by the 9/11 Commission as well as by this committee’s own investigations.

While it is true that FISA’s new collection authorities have made it a sword authorizing vast intelligence collection, returning FISA to the statute as it was written prior to 9/11 would be a mistake. Thankfully, that is not the only option. By making significant reforms to FISA that enhance transparency, ensure greater accountability to the rule of law, and protect privacy through innovative technology, Congress can help ensure FISA also remains a shield protecting American civil liberties.

¹ Remarks by the President on Securing Our Nation’s Cyber Infrastructure, May 29, 2009, available at http://www.whitehouse.gov/the_press_office/Remarks-by-the-President-on-Securing-Our-Nations-Cyber-Infrastructure (visited Sept. 25, 2013).

² See Bill Chappell, Snowden Is a Whistle-Blower, Americans Say in Poll, National Public Radio, July 10, 2013, available at <http://www.npr.org/blogs/thetwo-way/2013/07/10/200878660/snowden-is-a-whistle-blower-americans-say-in-poll> (visited Sept. 25, 2013).

³ James R. Clapper, “DNI Statement on Recent Unauthorized Disclosures of Classified Information,” June 6, 2013, available at

<http://iconthererecord.tumblr.com/tagged/declassified> (visited Sept. 23, 2013).

⁴ *In re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things From [Redacted]*, United States Foreign Intelligence Surveillance Court, No. BR 13-109, at 27 (Aug. 29, 2013) (internal quotation marks and citation omitted), available at

<http://www.uscourts.gov/uscourts/courts/fisc/br13-09-primary-order.pdf> (visited Sept. 25, 2013).

⁵ The National Security Agency: Missions, Authorities, Oversight and Partnerships, Aug. 9, 2013 (white paper), at p. 6, available at

http://www.nsa.gov/public_info/files/speeches/testimonies/2013_08_09_the_nsa_story.pdf (visited Sept. 25, 2013).

⁶ Sean Gallagher, “NSA ‘touches’ more of Internet than Google,” Ars Technica, Aug. 13, 2013, available at <http://arstechnica.com/information-technology/2013/08/the-1-6-percent-of-the-internet-that-nsa-touches-is-bigger-than-it-seems/> (visited Sept. 26, 2013).

⁷ This authority is often called “section 215” authority because it was added by section 215 of the USA Patriot Act; however, it is contained at section 501 of FISA. While section 501 of FISA predates 9/11, it was much narrower prior to the passage of the Patriot Act.

⁸ See, e.g. Michael Chertoff, NSA Surveillance Vital to Our Safety (Op-Ed), USA Today, Sept. 11, 2013, available at

<http://www.usatoday.com/story/opinion/2013/09/11/nsa-privacy-chertoff-911-column/2793063/> (visited Sept. 25, 2013).

⁹ See, e.g., Hearing of the Senate Judiciary Committee on Strengthening Privacy Rights and National Security: Oversight of FISA (Foreign Intelligence Surveillance Act) Surveillance Programs (July 13, 2013) (testimony of John C. Inglis, Deputy Director, National Security Agency), available at:

<http://iconthererecord.tumblr.com/post/57811913209/hearing-of-the-senate-judiciary-committee-on> (visited Sept. 25, 2013).

¹⁰ See id. (testimony of Sean M. Joyce, Deputy Director, Federal Bureau of Investigation).

¹¹ DNI Clapper Directs Annual Release of Information Related to Orders Issued Under National Security Authorities, Aug. 29, 2013, available at

<http://iconthererecord.tumblr.com/post/59719173750/dni-clapper-directs-annual-release-of-information> (visited Sept. 25, 2013).

¹² See *In re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things From [Redacted]*, supra note 4.

¹³ [Redacted], Memorandum Opinion, United States Foreign Intelligence Surveillance Court (Bates, J.) (Oct. 3, 2011) (“Bates October 2011 opinion”), available at <http://iconthererecord.tumblr.com/post/58944252298/dni-declassifies-intelligence-community-documents> (visited Sept. 25, 2013).

¹⁴ *In re Sealed Case No. 02-001*, Foreign Intelligence Surveillance Court of Review (2002), available at <https://www.fas.org/irp/agency/doj/fisa/fiscr111802.html> (visited Sept. 25, 2013).

¹⁵ Charlie Savage, “Roberts’s Picks Reshaping Secret Surveillance Court,” N.Y. Times, July 25, 2013.

¹⁶ See the multiple declassified opinions of the FISA court discussing this episode made available by the Director of National Intelligence. DNI Declassifies Intelligence Community Documents Regarding Collection Under Section 501 of the Foreign Intelligence Surveillance Act (FISA), Sept. 10, 2013, available at <http://icontherecord.tumblr.com/post/60867560465/dni-clapper-declassifies-intelligence-community> (visited September 25, 2013).

¹⁷ See Office of the Director of National Intelligence, 2012 Data Mining Report (April 12, 2013), pp. 6-7, available at <http://www.dni.gov/index.php/newsroom/reports-and-publications/193-reports-publications-2013/843-section-804-federal-agency-data-mining-report-2012> (visited Sept. 25, 2013).