Testimony and Statement for the Record of

Marc Rotenberg
Executive Director, EPIC
Adjunct Professor, Georgetown University Law Center

Hearing on
"The FISA Amendments Act of 2008"

Before the

House Committee on the Judiciary
Subcommittee on Crime, Terrorism, and Homeland Security

May 31, 2012
2141 Rayburn House Office Building
Washington, DC

Introduction

Mister Chairman and Members of the Subcommittee, thank you for the opportunity to testify today regarding the reauthorization of Title VII of the FISA Amendments Act of 2008 ("FAA"). My name is Marc Rotenberg, and I am President of the Electronic Privacy Information Center ("EPIC"). I also teach Information Privacy Law at Georgetown University Law Center, and I am a former chair of the ABA Committee on Privacy and Information Security.

EPIC is a non-partisan research organization, established in 1994 to focus public attention on emerging privacy and civil liberties issues. We work with a distinguished panel of advisors in the fields of law, technology, and public policy, and we have a strong interest in protecting the privacy of electronic communications. We have closely followed the developments of the Foreign Intelligence Surveillance Act ("FISA") and the Government's domestic and international surveillance activities. EPIC routinely reviews the annual reports concerning both Title III wiretap authority and FISA, and we have made recommendations to the Foreign Intelligence Surveillance Act Court of Review regarding that court's procedures.

We appreciate the Subcommittee's interest in the Foreign Intelligence Surveillance Act and its impact on important privacy interests.

Background

In my testimony today, I will review the key provisions of the FISA Amendment Act of 2008 ("FAA"),[1] discuss an important report from the American Bar Association ("ABA") on FISA reform, and make several recommendations to improve public accountability and oversight. In brief, I believe that requiring public dissemination of an annual FISA report, similar to reports for other forms of electronic surveillance, would improve Congressional and public oversight of the Government's information gathering activities. In addition, Congress should implement publication procedures for important decisions of the Foreign Intelligence Surveillance Court ("FISC"). At present, the FISA grants broad surveillance authority with little to no public oversight. To reauthorize the expansive provisions of Title VII of the FAA in their current form without improved transparency and oversight would be a mistake.

Passage of the FISA Amendments Act of 2008

The FISA Amendments Act of 2008, as adopted, clarified the legal basis for the use of electronic surveillance techniques by the Executive, but it also authorized surveillance of foreign communications, including communication of U.S. persons, on a mass scale without adequate public oversight. Among the achievements of the FAA was the recognition that federal statutes, such as FISA and ECPA, provide the exclusive authority for the Government's electronic surveillance activities. These statutory

[1] FISA Amendments Act of 2008, Title VII, 50 U.S.C. §§ 1881.

safeguards not only protect privacy, they also ensure the effective and efficient application of government resources to foreign intelligence gathering.

Section 702 of the FAA created new oversight mechanisms that require prior review the government surveillance and minimization procedures by the Foreign Intelligence Surveillance Court ("FISC").[2] The FAA prohibited surveillance of foreign targets as a pretext to conduct surveillance of persons within the United States, and added a new requirement of probable cause for surveillance of Americans abroad.[3]

However, section 702 of the FAA also gave the Government unprecedented authority to conduct electronic surveillance without first establishing probable cause to believe that a particular target was a foreign power or an agent of a foreign power. Instead, the FISC approves "certifications," submitted annually by the Attorney General and the Director of National Intelligence ("DNI"), which identify categories of foreign intelligence targets and describe minimization procedures and acquisition guidelines. The court's role in this process is merely to review the proposed procedures and guidelines, not to review the Government's actual surveillance practices. This procedure, which has the effect of a "rubber stamp," diminishes the independent role of the judiciary and leaves the executive with broad and minimally accountable collection authority.

Title VIII of the FAA also granted broad immunity to electronic service providers facilitating the Government's surveillance activities. This immunity was granted even though several alternative proposals would have provided adequate service provider protections for good faith compliance. While the companies were no doubt pleased to receive this broad immunity, the practical consequence was to further reduce the role of the courts and to diminish the opportunity for public oversight of FISA authorities.[4]

The 2003 ABA Resolution on FISA

Shortly after the attacks of September 11th, a special committee of the American Bar Association undertook an evaluation of the expanded use of the FISA, to ensure that Government conduct complied with constitutional principles while effectively and efficiently safeguarding national interests. The ABA report stressed the importance of both the Government's legitimate intelligence gathering activity and the protection of individuals from unlawful government intrusion. The ABA recommended that the Congress conduct regular and timely oversight, that FISA orders be sought only when the government has a "significant" foreign intelligence purpose, and that the Government

[2] 50 U.S.C. § 1881a.
[3] 50 U.S.C. § 1881b.
[4] This can be seen in the stark contrast between *Hepting v. AT&T*, 439 F. Supp. 2d 974 (N.D. Cal. 2006) (denying phone company's motion to dismiss customer action for constitutional and statutory violations related to warrantless surveillance programs), *Hepting v. AT&T*, 539 F.3d 1157 (9th Cir. 2008) (remanding to the district court in light of the FISA Amendments Act of 2008), and *In re Nat'l Sec. Agency Telecomms. Records Litig.*, 671 F.3d 881 (9th Cir. 2011) (upholding challenge to FAA telecommunications providers immunity under the Due Process clause).

make available an "annual statistical report on FISA investigations, comparable to the reports prepared by the Administrative Office of the United States Courts pursuant to 18 U.S.C. § 2519."[5]

This ABA report is particularly useful as the Congress now considers whether to renew the FISA Amendments Act, and the specific recommendation to provide an annual public report on FISA should be adopted.

The Need for Improved Reporting on FISA

Mr. Chairman, for almost twenty years, I have reviewed the annual reports produced by the Administrative Office of the US Courts on the use of federal wiretap authority as well as the letter provided each year by the Attorney General to the Congress regarding the use of the FISA authority.[6] EPIC routinely posts these reports when they are made available and notes any significant changes or developments.[7]

The report of the Administrative Office is remarkable document. I believe it is the most comprehensive report on wiretap authority produced by any government agency in the world. Pursuant to section 2519 of Title 18, the administrative office works closely with prosecutors and federal courts to provide a detailed overview of the cost, duration, and effectiveness of wiretap surveillance.[8] The report also breaks requests down into

---

[5] American Bar Association, *FISA Resolution*, February 10, 2003, *available at* http://epic.org/privacy/terrorism/fisa/aba_res_021003.html.

[6] *See, e.g.*, Administrative Office of the US Courts, *Wiretap Report 2010,* http://www.uscourts.gov/statistics/WiretapReports/WiretapReport2010.aspx; Letter from Assistant Attorney General Ronald Weich to Joseph Biden, President, United States Senate, Apr. 30, 2012 ("2011 FISA Annual Report to Congress"), http://www.fas.org/irp/agency/doj/fisa/2011rept.pdf.

[7] *See* EPIC, *Title III Wiretap Orders: 1968-2010*, http://epic.org/privacy/wiretap/stats/wiretap_stats.html; EPIC, *Foreign Intelligence Surveillance Act*, http://epic.org/privacy/terrorism/fisa/; EPIC, *Foreign Intelligence Surveillance Court (FISC)*, https://epic.org/privacy/terrorism/fisa/fisc.html.

[8] Section 2519 of Title 18 provides in full:

§ 2519. Reports concerning intercepted wire, oral, or electronic communications

(1) In January of each year, any judge who has issued an order (or an extension thereof) under section 2518 [18 USCS § 2518] that expired during the preceding year, or who has denied approval of an interception during that year, shall report to the Administrative Office of the United States Courts

(a) the fact that an order or extension was applied for;

(b) the kind of order or extension applied for (including whether or not the order was an order with respect to which the requirements of sections 2518(1)(b)(ii) and 2518(3)(d) of this title [18 USCS §§ 2518(1)(b)(ii) and 2518(3)(d)] did not apply by reason of section 2518(11) of this title [18 USCS § 2518(11)]);

(c) the fact that the order or extension was granted as applied for, was modified, or was denied;

(d) the period of interceptions authorized by the order, and the number and duration of any extensions of the order;

(e) the offense specified in the order or application, or extension of an order;

(f) the identity of the applying investigative or law enforcement officer and agency making the application and the person authorizing the application; and

useful statistical categories, including the type of crimes involved.[9] Such information is critical to evaluating both the effectiveness and the need for various types of Government surveillance activities.

We might disagree over whether the federal government engages in too much or too little electronic surveillance, but the annual report of the Administrative Basis provides a basis to evaluate the effectiveness of wiretap authority, to measure its cost, to even determine the percentage of communications captured that are relevant to an investigation. These reporting requirements ensure that law enforcement resources are appropriately and efficiently used while safeguarding important constitutional privacy interests.

By way of contrast, the Attorney General's annual FISA report provides virtually no meaningful information about the use of FISA authority other than the applications

---

(g) the nature of the facilities from which or the place where communications were to be intercepted.

(2) In March of each year the Attorney General, an Assistant Attorney General specially designated by the Attorney General, or the principal prosecuting attorney of a State, or the principal prosecuting attorney for any political subdivision of a State, shall report to the Administrative Office of the United States Courts--

(a) the information required by paragraphs (a) through (g) of subsection (1) of this section with respect to each application for an order or extension made during the preceding calendar year;
(b) a general description of the interceptions made under such order or extension, including (i) the approximate nature and frequency of incriminating communications intercepted, (ii) the approximate nature and frequency of other communications intercepted, (iii) the approximate number of persons whose communications were intercepted, (iv) the number of orders in which encryption was encountered and whether such encryption prevented law enforcement from obtaining the plain text of communications intercepted pursuant to such order, and (v) the approximate nature, amount, and cost of the manpower and other resources used in the interceptions;
(c) the number of arrests resulting from interceptions made under such order or extension, and the offenses for which arrests were made;
(d) the number of trials resulting from such interceptions;
(e) the number of motions to suppress made with respect to such interceptions, and the number granted or denied;
(f) the number of convictions resulting from such interceptions and the offenses for which the convictions were obtained and a general assessment of the importance of the interceptions; and
(g) the information required by paragraphs (b) through (f) of this subsection with respect to orders or extensions obtained in a preceding calendar year.

(3) In June of each year the Director of the Administrative Office of the United States Courts shall transmit to the Congress a full and complete report concerning the number of applications for orders authorizing or approving the interception of wire, oral, or electronic communications pursuant to this chapter [18 USCS §§ 2510 et seq.] and the number of orders and extensions granted or denied pursuant to this chapter [18 USCS §§ 2510 et seq.] during the preceding calendar year. Such report shall include a summary and analysis of the data required to be filed with the Administrative Office by subsections (1) and (2) of this section. The Director of the Administrative Office of the United States Courts is authorized to issue binding regulations dealing with the content and form of the reports required to be filed by subsections (1) and (2) of this section.

[9] 18 U.S.C. § 2519(1)(e).

made by the government to the Foreign Intelligence Surveillance Court.[10] There is no information about cost, purposes, effectiveness, or even the number of non-incriminating communications of US persons that are collected by the government. Moreover, under the new procedures that authorize programmatic surveillance without a specific target, it is almost impossible to assess and compare the aggregate numbers since passage of the FAA. And while we acknowledge a 2006 amendment to the FISA reporting that now includes the numbers of National Security Letter requests made by the FBI concerning US persons, without more information it is very difficult to assess the significance of this number. Again by way of contrast, the reports prepared by the Department of Justice Inspect General concerning the misuse of NSL authority provide a great deal of information, but these reports are not prepared annually. So, while FISA authority remains in place and NSL authority remains in place, there is little information available to Congress or the public beyond the absolute numbers involved in the use of these authorities.

We recognize that section 702 contains internal auditing and reporting requirements. The Attorney General and DNI assess compliance with targeting and minimization procedures every six months, and provide reports to the FISC, congressional intelligence committees, and the Committees on the Judiciary.[11] The inspector general of each agency authorized to acquire foreign intelligence information pursuant to FISA must submit similar semiannual assessments. The head of each authorized agency must also conduct an annual review of FISA-authorized "acquisitions" and account for their impacts on domestic targets and American citizens.[12] Yet none of this information is made available to Congress or the public broadly, and no public oversight has occurred. There is simply no meaningful public record created for the use of these expansive electronic surveillance authorities.

Similar internal auditing procedures have failed in the past, and Congress would be wise to take the opportunity of the review of the FAA to establish more robust public reporting requirements and oversight procedures.[13]

The use of aggregate statistical reports has provided much needed public accountability of federal wiretap practices. These reports allow Congress and interested groups to evaluate the effectiveness of Government programs and to ensure that

---

[10] It is clear from the Attorney General's annual reports that FISC applications are routinely approved with very rare exceptions. *See Amnesty Int'l USA v. Clapper*, 638 F.3d 118, 140 (2d Cir. 2011) ("Empirical evidence supports this expectation: in 2008, the government sought 2,082 surveillance orders, and the FISC approved 2,081 of them."). Of the Government's 1,676 requests to the FISC for surveillance authority in 2011, none were denied in whole or in part. *See* 2011 FISA Annual Report to Congress, *supra*, note 6.

[11] 50 U.S.C. § 1881a(j)(1).

[12] 50 U.S.C. § 1881a(j)(3).

[13] The warrantless wiretapping program continued for several years because the government failed to routinely inform the Foreign Intelligence Surveillance Court of its activities. And the public was also kept in the dark. *See* James Risen & Eric Lichtblau, *Bush Lets U.S. Spy on Callers Without Courts*, N.Y. Times, Dec., 16, 2005, at A1, *available at* http://www.nytimes.com/2005/12/16/politics/16program.html.

important civil rights are protected. Such reports do not reveal sensitive information about particular investigations, but rather provide aggregate data about the Government's surveillance activities. That is the approach that should be followed now for FISA.

Transparency is Necessary for Adequate Oversight: *Clapper v. Amnesty Int'l USA*

It is against this background that the Supreme Court recently decided to review *Clapper v. Amnesty Int'l USA*, an important case challenging the FAA. The question presented in *Clapper* is whether individuals who live in the United States and frequently communicate internationally have Article III standing to challenge the Government's surveillance activities pursuant to FISA based on a reasonable fear that their private communications are being intercepted.[14]

While some scholars have expressed sympathy for the government's position in *Clapper*, suggesting that it is too speculative to allow parties to sue when they have failed to establish that the surveillance occurred,[15] others have noted that the plaintiffs can likely establish the necessary "fear of future injury and costs incurred to avoid that injury" necessary under Article III.[16] Additionally, a lack of transparency or knowledge of the extent of government surveillance can have a severe chilling effect on protected speech and public activity. Individuals who are not reasonably certain that their communications will be private and confidential could be forced to censor themselves to protect sources and clients. This broad chilling effect is an injury in and of itself, regardless of the specific unlawful interception of private communications.

Given the lack of transparency and FISA reporting, it seems eminently reasonable for these individuals to fear unlawful interception of their private communications. In the absence of public reporting, similar to the annual reports provided for Title III Wiretaps, Americans are understandably concerned about the scope of surveillance pursued under the FISA.

The most obvious reason for this is that electronic surveillance is difficult to detect. Unlike physical entry into a home or the seizure of private property, electronic surveillance routinely occurs without any noticeable disturbance to the target or to innocent bystanders whose personal communications are intercepted. Federal Wiretap law traditionally addressed this problem by establishing Government notification requirements, once an investigation is closed, to those who had been the subject of surveillance.[17] These notification procedures helped ensure accountability. However,

---

[14] *See Amnesty Int'l USA v. Clapper*, 638 F.3d 118 (2d Cir. 2011), *reh'g denied*, 667 F.3d 163, *cert. granted*, 132 S. Ct. ____, 2012 WL 526046 (2012).

[15] Orin Kerr, *Amnesty International USA v. Clapper and Standing to Challenge Secret Surveillance Regimes*, Volokh Conspiracy (Mar. 24, 2011, 2:46 AM).

[16] Steve Vladeck, *Why Clapper Matters: The Future of Programmatic Surveillance*, Lawfare (May 22, 2012, 10:13 AM), http://www.lawfareblog.com/2012/05/clapper-and-the-future-of-surveillance/.

[17] *See* 18 U.S.C. § 2518(8)(d) (Wiretap Act notification provision); 50 U.S.C. § 1806(c) (FISA notification provision).

there has clearly been a move by the government, post 9/11, to move away from subject notification. In this respect, the FAA has done much to undermine the means of accountability that existed previously which helped ensure accountability

Congress should not reauthorize Title VII of the FAA without adequate transparency and oversight procedures in place.

The Need for Increased FISC Oversight Authority and Transparency

In addition to the Government's FISA activities, Congress should be concerned with the transparency of the FISC itself, and its authority to oversee Government surveillance procedures. Often referred to as a secret court, the FISC rarely publishes any substantive information regarding the cases and controversies that are heard by its judges; only a handful of written opinions have been released since the Court's inception, and little else, despite the potential for these types of Court documents to provide valuable guidance on the Court's purpose and function.

The public remains concerned by the secrecy that surrounds the FISC and its proceedings. The sensitive nature of the proceedings that come in front of the FISC must protect national security and provide notice to the individual targeted by the proceeding, at an appropriate time.[18] Currently, the FISC is only required to report on the number of orders it issues and denies: no other information accompanies the annual report and the public receives no other information about what cases come before the court each year. The only information currently available about the FISC on the U.S. Courts website is its adopted rules of procedure from November 2010.[19]

Any renewal of the FAA must take account of this lack of transparency and provide some assurance that the FISC can conduct sufficient oversight of Government surveillance activities. This could include public reporting procedures for FISC opinions, published statistics for FISC orders, and a provision for an increased web presence, or other source of data that can be easily accessed. It is important to provide the public with information about the Court, without compromising the government's security and intelligence gathering interests. Such information could include an overview of the Courts docket and the identity of the judge who is assigned to each case. The best way to increase public understanding of the FISC would be to publish past orders and opinions. Publishing such opinions while redacting sensitive materials would provide increased accountability for an important executive branch function.

[18] Foreign Intelligence Surveillance Act, 50 U.S.C. § 1806.

[19] *See* U.S. Foreign Intelligence Surveillance Court, *Rules of Procedure*, Nov. 1, 2010, *available at* http://www.uscourts.gov/uscourts/RulesAndPolicies/rules/FISC2010.pdf. *See also* EPIC, *Comments to Proposed Amended FISC Rules* (Oct. 4, 2010), http://epic.org/privacy/terrorism/fisa/EPIC%20Comments_FISC%202010%20Proposed%20Rules.pdf.

Conclusion

In the lead up to the passage of the FISA Amendments Act of 2008, there was much discussion of the need to "balance" national security and privacy interests. But the better way to understand the challenge facing Congress may be to think in terms of the need to establish a counter-balance. Where the government is given new authorities to conduction electronic surveillance, there should be new means of oversight and accountability. The FISA Amendments Act failed this test. There is simply too little known about the operation of the FISA today to determine whether it is effective and whether the privacy interests of Americans are adequately protected. Before renewing the Act, we urge the committee to carefully assess these new procedures and to strengthen the oversight mechanisms by (1) improving public reporting requirements, and (2) strengthening the authority of the FISA Court to review the government's use of FISA authorities.

Thank you again for the opportunity to testify today. I would be pleased to answer your questions.