Prepared Statement for the Record of

Marc Rotenberg, President
Electronic Privacy Information Center

Workshop on

Domestic Surveillance Programs Operated Under the USA PATRIOT Act and the Foreign Intelligence Surveillance Act

Before the

Privacy and Civil Liberties Oversight Board

Renaissance Mayflower Hotel
Washington DC
July 9, 2013

My name is Marc Rotenberg. I am President and Executive Director of the Electronic Privacy Information Center in Washington, DC. I am also on the faculty at Georgetown University Law Center where I have taught the Law of Information Privacy for more than twenty years. I have served as Chair of the ABA Committee on Privacy and Information Security.

EPIC is a public interest research center in Washington, D.C. established in 1994 to focus public attention on emerging civil liberties issues and to protect constitutional values and the rule of law. EPIC has extensive expertise with the Foreign Intelligence Surveillance Act ("FISA") and the Foreign Intelligence Surveillance Court ("FISC"), and we have routinely reviewed the annual report. We also worked with an ABA Committee almost ten years ago to recommend improvements in reporting for FISA activity.

I want to begin by thanking the Civil Liberties Board for convening this important public meeting today. There are few times in recent history when the American public has expressed more concern about privacy than it has today. And underlying the concern about privacy is a deeper concern – did the US government act lawfully when it obtained so much information about so many American citizens without any ties to terrorists or criminal conduct? It is that question that I hope your committee will be able to answer.

I will today briefly outline steps that EPIC has taken to respond to the National Security Agency's ("NSA") domestic surveillance program, answer the questions you have asked about surveillance and technology, and make certain recommendations for the Oversight Board.

Regarding the focus of your workshop today and certain provisions of the Foreign Intelligence Surveillance Act. I also want to mention that early in my studies of privacy, I reviewed the reports of the Church Committee and had the opportunity to meet with Senator Church in Washington, DC shortly after the work of his committee was completed. I believe Senator Church would find it inconceivable that after the passage of the Foreign Intelligence Surveillance Act, the extraordinary powers of the NSA could be directed toward the American public. It is almost exactly against this outcome that his efforts and the FISA were directed.

I. EPIC's Actions to Date

I would like to call the Oversight Board's attention to several actions that EPIC has undertaken to address the concerns arising from the government's domestic surveillance program. All of these steps are intended to ensure a more fully informed public debate and may be relevant as your work goes forward.

First, this week EPIC filed a mandamus petition with the US Supreme Court, alleging that the Foreign Intelligence Surveillance Court exceeded its authority when it compelled Verizon to produce all of the call detail records of its telephone customers to

the NSA.[1] In our view, it is simply impossible for the Federal Bureau of Investigation ("FBI") to have satisfied the necessary elements of section 215 that would have allowed this unbounded disclosure to occur. We believe the Court must therefore vacate the order issued by the FISC.

Second, EPIC has formally petitioned General Alexander to begin a public comment process on the NSA's domestic surveillance program.[2] It is our view that the agency has engaged in substantial change in agency practice that requires a formal notice and comment rulemaking. 32 legal scholars and technology experts signed our initial petition. It has since been joined by several thousand individuals. EPIC intends to renew the petition each week until the agency responds. Even the NSA does not operate outside the requirements of the Administrative Procedures Act

Third, EPIC has asked the Commissioners of the Federal Communications Commission to determine whether Verizon violated Section 222 of the Telecommunications Act of 1996 when it disclosed the complete call details records of all its US customers.[3] The FCC has jurisdiction over the Telecommunications Act and is responsible for regulating the business practices of telecommunication firms operating within the United States.

Fourth, EPIC has filed several FOIA requests to obtain the legal interpretation of the legal authorities under consideration at this hearing.[4] As many others have pointed out, it is highly unusual to have secret legal authorities in the United States. With respect to the routine access of the telephone logs of Americans, it is absolutely without precedent.

We are also pursuing FOIA requests for document regarding US officials who lobbied against efforts by the EU government to strengthen their privacy safeguards. As you aware, the news about PRISM has sparked a privacy backlash in Europe and undermined the position of US negotiators entering important trade negotiations. We wish to know whether the position of the US officials who opposed the EU privacy laws was directed, in part, by the demands of the National Security Agency

III. Technology, Surveillance, and Privacy

This panel focuses on the role of technology, specifically the problem of metadata. On this issue, I will make four points: (1) the law has been turned upside down; (2) the data is far more detailed than most people understand or the government will

[1] *In Re Electronic Privacy Information Center*, Petition for a Writ of Mandamus, *available at* http://epic.org/EPIC-FISC-Mandamus-Petition.pdf.
[2] Petition from EPIC to General Keith Alexander and Secretary Chuck Hagel, *available at* http://epic.org/NSApetition/.
[3] EPIC Complaint to the FCC (June 11, 2013), *available at* http://epic.org/privacy/terrorism/fisa/EPIC-FCC-re-Verizon.pdf.
[4] *See, e.g.*, EPIC FOIA Request to Office of Information Policy, Dep't of Justice (June 7, 2013), *available at* http://epic.org/EPIC_FOIA_Request_NSA_Verizon_DOJ.PDF (concerning section 215 legal interpretation).

concede; (3) the metadata is combined with other data to create detailed profiles of individuals and the relationships between individuals; and (4) legal solutions are needed.

(1) The Law Has Been Turned Over and Extended Beyond Recognition

The law of the United States has been turned upside down and consequently the rule of law has been undermined. FISA is a law focused on protecting Americans against the excesses of foreign surveillance, but it is now used through section 215 to perform purely domestic surveillance. Furthermore, much of the law that interprets FISA as well as the Patriot Act is completely secret. The use of section 215 to perform domestic surveillance exceeds its statutory authority and the secret interpretation of law to stretch it beyond conceivable bounds is directly at odds with a democracy.

The government cites *Smith v. Maryland*[5] for the proposition that there is no reasonable expectation of privacy in metadata.[6] The case focused on the recording of phone numbers coming and going from one specific phone. At the time the Supreme Court ruled on collecting phone numbers via pen registers in *Smith v. Maryland*, metadata created very few details when using the phone and very few activities created metadata. Today, the situation is reversed—most activities do create very detailed metadata. The government, in secret, stretched the *Smith v. Maryland* ruling on collection of minimal metadata from one specific phone number to the collection of detailed call records of all Americans.

(2) Metadata is Far More Detailed Then the Government Admits

The Director of National Intelligence recently apologized for an answer he gave at an oversight hearing regarding whether the NSA collects "any type of data at all on millions or hundreds of millions of Americans." His answer was clearly wrong but more significant may be the NSA talking point that the Verizon Order only authorizes the collection of "barebones records."[7]

Call detail records collected under the Verizon Order are not bare bone records. They are extensive accounts of each call that includes the number dialed, the time of the call, the duration of the call, the cell towers used to complete the call, and the unique identifiers of the mobile phone and subscriber to the network. The combination of metadata collected by phone records can be directly linked to each user's identity and reveal her contacts, clients, associates, location, movement over time, and personal activities.

---

[5] 442 U.S. 735 (1979).

[6] *See* Memorandum from Kenneth L. Wainstein, Assistant Attorney General, National Security Division to Michael B. Mukasey, Attorney General, and Dr. Robert Gates, Secretary of Defense, regarding Proposed Amendment to Department of Defense Procedures to Permit the National Security Agency to Conduct Analysis of Communications Metadata Associated with Persons in the United States (November 20, 2007) [hereinafter *2007 AG Memo*], *available at* http://s3.documentcloud.org/documents/717974/nsa-memo.pdf.

[7] FISA/NSA Talking Points, *available at* https://s3.amazonaws.com/s3.documentcloud.org/documents/713590/fisa-business-records-talking-points-6-6-13.pdf.

The amount of detailed metadata we create is steadily increasing leaving the door open for an escalation in evasive surveillance through metadata analysis. Our lives will increasingly involve actions that create metadata telling a story about everything we do, where we do it, and whom we interact with when we do it.

(3) Metadata, Technology, and Function Creep

The government uses what it calls "contact chaining" to organize the communications metadata it collects. Contact chaining consist of the use of computer algorithms to identify the first tier of contacts a specific phone number has been in contact with or attempted to contact. The same process is run on the first tier contacts and then the second tier contacts and so forth and so on.[8] The process provides a comprehensive picture of the contacts connected to a phone number that can easily be cross-referenced with a multitude of databases collected by the government.

In addition to the database of phone records, the NSA maintains "records of telephone numbers and electronic communications accounts/addresses/identifiers that NSA has reason to believe are used by United States persons."[9] The government also collects a number of other databases with information on US persons in the name of national security. For example, the Department of Homeland Security collects travel records on all airline passengers, and the Federal Bureau of Investigation is in the process of creating a massive biometric database. These databases along with many others can be copied by the National Counterterrorism Center for their own use.

Technology is advancing towards more surveillance and data collection as more and more items we interact with on a daily basis become internet-enabled.[10] As more data is collected and computer algorithms advance to better unearth hidden correlations in large datasets, the pressure within the intelligence community will be great to use databases in new ways to mind for more information.[11]

No amount of technology will stop the inevitable pressure to use the information collected by the NSA specifically and the government generally in cutting-edge ways. Function creep is inevitable as technology advances and future possibilities become

[8] *2007 AG Memo.*
[9] Eric H. Holder, Jr., Attorney General, *Procedures Used by the National Security Agency for Targeting Non-United States Persons Reasonably Believed to be Located Outside the United States to Acquire Foreign Intelligence Information Pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, as Amended*, *avaialbe at* http://s3.documentcloud.org/documents/716633/exhibit-a.pdf.
[10] Bruce Schneier, *Will Giving the Internet Eyes and Ears Mean the End of Privacy*, The Guardian, May 16, 2013, *available at* http://www.guardian.co.uk/technology/2013/may/16/internet-of-things-privacy-google (highlighting the ubiquitous surveillance coming from the Internet of Things).
[11] *See* Laura K. Donohue, *Anglo-American Privacy and Surveillance*, 96 J. CRIM. L. & CRIMINOLOGY 1059, 1144-1153 (2006) (describing the extensive use of government databases and private sector data for data mining).

today's reality. For example, the FBI now uses facial recognition technology to compare suspects in investigations to the photo records kept by many state DMVs.[12]

(4) Legal Solutions are Needed to Protect Privacy

Many have proposed the adoption of new techniques to protect privacy. EPIC has supported many of these recommendations, including more robust techniques for secure communications, anonymization, minimization, and deindentification. In fact, EPIC began with the first Internet petition, which concerned the freedom to use encryption. But we and leading computer scientists have also recognized the limitations of these techniques. Groups such as the ACM routinely advise Congress about the limitations of these technologies.

Perhaps the view was expressed most clearly by former MIT President and former Presidental Science Advisor Jerome Wiesner. Professor Wiesner had been asked to speak before Congress on personal privacy and technology. This is what he said:

> There are those who hope new technology can redress these invasions of personal autonomy that information technology now makes possible, but I don't share this hope. To be sure, it is possible and desirable to provide technical safeguards against unauthorized access. It is even conceivable that computers could be programmed to have their memories fade with time and to eliminate specific identity. Such safeguards are highly desirable, but the basic safeguards cannot be provided by new inventions. They must be provided by the legislative and legal systems of this country. We must face the need to provide adequate guarantees for individual privacy.[13]

In the end, there is no silver bullet that assures the protection of national security and safeguards civil liberties. The solutions are ultimately found in law and public policy, and they should reflect the principles of a Constitutional democracy.

IV. Recommendations

Since 9/11 there has been much discussion of the need to "balance" national security and privacy interests in the United States. The better way to understand the challenge facing lawmakers in a Constitutional democracy is the need to establish a "counter balance." Where the government is given new authorities to conduct surveillance, there should be new means of oversight. Based on what we have learned, it is clear that the system of oversight for the collection of foreign intelligence information has collapsed. There is no meaningful review.

---

[12] EPIC: FBI Performs Massive Virtual Line-up by Searching DMV Photos, http://epic.org/2013/06/fbi-performs-massive-virtual-l.html.

[13] *Federal Data Banks, Computers and the Bill of Rights: Hearings Before the Subcomm. On Constitutional Rights of the House Comm. on the Judiciary*, 92d Cong., 1st Sess. Part I, 761-774 (1971) (testimony of Jerome B. Wiesner, provost elect, Massachusetts Institute of Technology).

EPIC recommends that the PCLOB:

1. Reject the view that FISC currently has the authority to issue such unbounded requests for personal data as are found in the Verizon Order. The program is unlawful and the orders of the FISC that sustain the program should be vacated.

2. Recommend improvements in public reporting for FISA similar to those requirements contained in the federal Wiretap Act, which includes the following:
    a. Judges must report the duration of the wiretap order, specific offense specified in application, identity of party applying, the person authorizing wiretap, and the nature of the facilities to be wiretapped.[14]
    b. Attorney Generals must report the nature and frequency of incriminating information obtained from wiretap, the number of persons whose communications were intercepted, and the number of arrests, trials, motions to suppress evidence, and convictions resulting from intercepted communications.[15]

3. Support efforts to safeguard personal information and minimize the data collected by the federal government but recognize also the limitations of these techniques and the need to establish better oversight, transparency, and accountability

4. Reconsider the scope of legal protection for "meta data" in light of the actual scope of the government's activities and the Court's recent decisions in *United States v. Jones*, 132 S. Ct. 945 (2012); *Clapper v. Amnesty International*, 133 S. Ct. 1138 (2013); *Maryland v. King*, 133 S. Ct. 1958 (2013); and *Florida v. Jardines,* 133 S. Ct. 1409 (2013). In EPIC's view, the NSA's domestic surveillance program is constitutionally impermissible. Given the opportunity to address this question, we believe that the Supreme Court would reach a similar conclusion.

Thank you for the opportunity to appear before the Board today.

[14] 18 U.S.C. 2519.
[15] *Id.*