Deutscher Bundestag

1st Committee of Inquiry

in the 18th electoral term

Hearing of Experts

"Surveillance Reform After Snowden"

September 8, 2016

Written Statement of

Timothy H. Edgar

Senior Fellow

Watson Institute for International and Public Affairs

Brown University

Providence, Rhode Island

United States of America

Prof. Dr. Patrick Sensburg, MdB, and Members of the Committee:

Thank you for the opportunity to testify on the topic of the reforms the United States government has made to its surveillance laws and policies in the wake of the revelations of Edward Snowden concerning signals intelligence collection.[1]

Before a crowd of tens of thousands in Berlin during in the summer of 2008, a young senator from Illinois and candidate for President, Barack Obama, drew cheers when he promised a more cooperative relationship with the world. Obama made the case for "allies who will listen to each other, who will learn from each other – who will, above all, trust each other."[2] In 2013, Germans were not happy when they found out just how President Obama's intelligence community had been listening.

The good news is that in the past three years we have seen substantial reforms in intelligence practices. President Obama's legacy will include the most significant reforms in almost four decades of the laws and polices that govern collection of

[1] This statement contains my personal views only. It does not reflect the views or policies of the United States government. It has been reviewed by the Office of the Director of National Intelligence to ensure it does not contain classified information.
[2] Jonathan Freedland, *US Elections: Obama wows Berlin crowd with historic speech*, THE GUARDIAN, July 24, 2008, available at http://www.theguardian.com/global/2008/jul/24/barackobama.uselections2008 (visited Apr. 8, 2016).

signals intelligence by American intelligence agencies, including the National Security Agency (NSA).

My perspective on the issue of privacy and intelligence surveillance is shaped by my unique experience. From 2001 to 2006, I was the legislative counsel for national security for the American Civil Liberties Union – one of largest and oldest non-governmental organizations in the world with a mission of defending fundamental rights. As an ACLU lawyer, I argued against many of the counterterrorism policies adopted by the administration of George W. Bush that we believed posed a threat to privacy and other civil liberties.

In early 2006, I was offered a unique position safeguarding civil liberties in the office that oversees the United States intelligence community – the Office of the Director of National Intelligence. From 2006 to 2013, I quietly worked with other lawyers and privacy officials inside the United States government in a new office with oversight of surveillance programs.

As surprised as I was by the breadth of NSA surveillance, I was just as surprised by how seriously everyone inside the government took the rules that govern it. The problem was that these rules, designed in the 1970's to prevent "spying on Americans," had become inadequate for the digital age. While many inside the intelligence community understood this, our efforts to launch a meaningful dialogue with civil society on issues of privacy were complicated by the demands of secrecy.

After six years and two administrations, I left my government position to pursue research and teaching. In June 2013, I accepted a full-time position at Brown, helping launch a new degree program in cybersecurity. Only a few days after my formal resignation, a young government contractor, Edward Snowden, chose to reveal the details of NSA surveillance to the world, including many of the programs on which I had worked.

Snowden's decision precipitated the open debate on privacy and surveillance we sorely needed but never had. The debate has already forced change.

- Under the leadership of President Obama, the intelligence community has launched a transparency drive. The Director of National Intelligence has released thousands of pages of once-classified documents using an innovative platform, a tumblr website called "IC on the record," in the interests of transparency. Although many assume that all public knowledge of NSA spying programs came from Snowden's leaks, many of the revelations in fact came from IC on the Record. The Obama administration has instituted other mechanisms, including an annual surveillance transparency report.[3]

[3] *See* ODNI Calendar Year 2014 Transparency Report – Statistical Transparency Report Regarding Use of National Security Authorities, Apr. 22, 2015, available at http://icontherecord.tumblr.com/transparency/odni_transparencyreport_cy2014 (visited Apr. 15, 2016).

- For the first time ever, intelligence agencies have adopted rules to protect the privacy of foreign citizens. Presidential Policy Directive 28 (PPD-28) extends minimization and retention requirements that once applied only to information belonging to United States persons (citizens and legal residents) to all personal information. PPD-28 provides that "All persons should be treated with dignity and respect, regardless of their nationality or wherever they might reside, and all persons have legitimate privacy interests in the handling of their personal information." It requires "appropriate safeguards for the personal information of all individuals" in signals intelligence activities "regardless of the nationality of the individual to whom the information pertains or where that individual resides." While the rules are admittedly modest, the concept is revolutionary.[4]

- Congress has ended the bulk collection of American telephone records. The USA FREEDOM Act, enacted in 2015, replaces that program with an

[4] *Presidential Policy Directive – Signals Intelligence Activities (Presidential Policy Directive 28/PPD-28)* at § 4, Jan. 17, 2014, available at https://www.whitehouse.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities (visited Feb. 21, 2016). All intelligence agencies have now issued new procedures, or revised existing procedures, to fulfill this requirement. *See* Office of the Director of National Intelligence, *Signals Intelligence Reform: 2015 Anniversary Report*, available at https://icontherecord.tumblr.com/ppd-28/2015/privacy-civil-liberties#ppd-28 (visited Sept. 3, 2015).

alternative arrangement in which the data remains with the companies, subject to query by NSA analysts.[5]

- The Foreign Intelligence Surveillance Court has appointed a panel of cleared outside lawyers to provide an independent voice in its secret proceedings. These include some of the finest national security lawyers in the United States, with a record of challenging NSA programs.[6]

- The Court of Justice of the European Union has struck down transfers of personal data to American companies. In response, the United States has negotiated a new agreement, the "Privacy Shield," to give Europeans some ability to challenge the use of their personal data. While I believe the Privacy Shield is not sufficient to address the CJEU's concerns about either the standard for surveillance or redress for EU citizens, the process shows that the United States is listening to European concerns. The engagement of the

[5] Uniting and Strengthening America by Fulfilling Rights and Ensuring Effective Discipline Over Monitoring Act (USA FREEDOM Act) of 2015, Pub. L. No. 114-23, 129 Stat. 268 (June 2, 2015).

[6] Section 401 of the USA FREEDOM Act sets forth the process for appointment of amici curiae to the courts established by the Foreign Intelligence Surveillance Act. The Foreign Intelligence Surveillance Court announced its list of amici in November 2015. *See* Cody M. Poplin, "Amici Curiae for FISC Announced," *Lawfare (blog)*, Dec. 1, 2015, available at https://www.lawfareblog.com/amici-curiae-fisc-announced (visited Sept. 3, 2016). It has since taken advantage of this provision. *See, e.g., Memorandum Opinion and Order* at pp. 5-7 (For. Intel. Surv. Ct. Nov. 6, 2015) (appointment of Amy Jeffress), available in declassified form at https://www.dni.gov/files/documents/20151106-702Mem_Opinion_Order_for_Public_Release.pdf (visited Sept. 3, 2016).

US intelligence community is also a hopeful sign. The Privacy Shield agreement will be certainly be tested in European courts.[7]

Taken as a whole, these changes amount to a new reform era for intelligence surveillance.

Still, there is much more to do. Next year, a new president and a new Congress will again confront the issue of surveillance. At the end of 2017, the authority the NSA uses to compel the collection of Internet and other communications from American companies will expire. The expiration of section 702 of the Foreign Intelligence Surveillance Act – which provides authority for the NSA's PRISM and "upstream collection" programs – will give a new administration a chance to go further in the direction of reforming surveillance.[8]

---

[7] *See Maximillian Schrems v. Data Protection Commissioner* (Court of Justice of the European Union Oct. 6, 2015), no. C-362/14, Judgement of the Court (Grand Chamber), available at http://curia.europa.eu/juris/documents.jsf?num=C-362/14 (visited Jan. 21, 2016). In July 2016, the United States and European Union announced the creation of the "Privacy Shield" framework, in response to the *Schrems* decision. The Privacy Shield documents include two letters from the Office of the Director of National Intelligence that detail the safeguards that apply to foreign intelligence collection under US law, including the reforms instituted in the aftermath of the Snowden revelations. *See* International Trade Administration, United States Department of Commerce, *EU-U.S. Privacy Shield Framework*, available at https://www.privacyshield.gov/EU-US-Framework (visited Sept. 3, 2016).

[8] The law that authorizes PRISM and "upstream collection" is section 702 of the Foreign Intelligence Surveillance Act, 50 U.S.C. § 1881(a), which was added by the FISA Amendments Act of 2008, Pub. L. No. 110-261, 122 Stat. 2436 (July 20, 2008). Section 702 was reauthorized in 2012. *See* FISA Amendments Act Reauthorization Act of 2012, Pub. L. No. 112-238, 126 Stat. 1631 (Dec. 30, 2012). The law now expires on December 31, 2017.

In "Go Big, Go Global: Subject the NSA's Overseas Programs to Judicial Review," I propose a three step process for bringing the NSA's global surveillance out of the shadows and into the digital age. The full paper is attached.

To summarize:

- First, all NSA surveillance programs (with a few exceptions) should be subject to judicial review under the Foreign Intelligence Surveillance Act.

- Second, the United States should limit its surveillance of the citizens of friendly democratic nations (such as Germany) to international terrorism and other specific security threats – but only if those countries agree to limit their intelligence practices on a reciprocal basis. Judicial review could make such an agreement credible and enforceable.

- Third, Congress should provide that signals intelligence programs be subject to meaningful challenge in the federal courts by those who reasonably fear surveillance, even if they cannot show their communications have actually been intercepted.

Note that this last proposal would bring American law closer to the way international human rights law treats the issue of injury, as outlined in the 1978

case of *Klass v. Germany.*[9] While Article III of the United States Constitution, as interpreted by the United States Supreme Court in the 2013 case of *Clapper v. Amnesty International*,[10] poses a challenge to such an approach, I believe there are viable ways Congress could broaden the ability of human rights organizations to challenge mass surveillance practices.

Thank you again, and I welcome your questions.

[9] *Klass and others v. Federal Republic of Germany* (European Court of Human Rights Sept. 6, 1978), Series A, No. 28, 2 EHRR 214, at ¶¶ 30, 34-38, available at http://www.hrcr.org/safrica/limitations/klass_germany.html (visited Jan. 21, 2016).

[10] *Clapper v. Amnesty International*, 568 U.S. __, No. 11-1025 (Feb. 26, 2013).