stiftung | neue verantwortung

Committee of Inquiry of the German Parliament
Expert Statement
Ben Scott
15 July 2015

Table of content

Introduction

The disclosures of NSA documents by Edward Snowden in June 2013 opened a heated debate about human rights and civil liberties in the digital age -- not just in Berlin and Brussels, but also in Washington. Political, business and civil society leaders from across the world joined calls for rapid changes in law and policy to address these problems both in the United States and in their home countries. Yet, two years later -- despite knowing far more about who, how, and what surveillance is being done -- there have been no sweeping changes to law and policy in any country. Germany is among the only nation still publicly challenging the US and the UK to change their ways. None have attempted to lead reform efforts by example. Most countries have made a quiet accommodation. Others are responding to security threats by liberalizing rather than tightening surveillance law.[1]

Yet, the story has not faded away. The headlines continue, documenting with leaked classified materials the details of the NSA's reach into the communications networks of friends and foes alike. Meanwhile, the German-led investigations into these matters -- including the one propelled by this committee -- have primarily revealed new information about BND complicity in digital surveillance rather than new details about the NSA. Two years after Snowden, the story is not simply about the power of the American signals intelligence. It is a complex history of interlocking agencies, cooperative surveillance operations, asymmetrical intelligence sharing, and wide gaps between what security agencies are doing and what elected officials (and their publics) know about it. The latest allegations now suggest that the NSA's target lists within the German government extended well beyond the Chancellor.[2] But so too is the BND accused of enabling or actively intercepting communications between neighboring European states.[3] And there is little doubt that cooperation between the BND and NSA is extensive.[4]

The experience of the last two years yields an unsettling conclusion for many: even the unprecedented scope and political shock of the Snowden disclosures will not deliver rapid and robust reform of security and privacy policy in democratic states. Therefore, it is easy to reach a cynical conclusion that there will be no change and the breakdown in trust between allies will be left unmended. But there are reasons for optimism in the longer term.

---

[1] Martin Untersinger, "If You Can't Beat 'Em: France, Up In Arms Over NSA Spying, Passes New Surveillance Law", *The Intercept*, 24. Juni 2015, https://firstlook.org/theintercept/2015/06/24/france-protests-nsa-spying-passes-new-surveillance-law/

[2] Georg Mascolo, et al., "Von Kohl bis Merkel - die NSA hörte mit", *Süddeutsche.de*, 8. Juli 2015, http://www.sueddeutsche.de/politik/wikileaks-dokumente-von-kohl-bis-merkel-die-nsa-hoerte-mit-1.2556461

[3] Gerald Traufetter, "BND-Affäre: Österreichischer Abgeordneter zeigt Telekom und BND an", *Spiegel.de*, 18. Mai 2015, http://www.spiegel.de/netzwelt/netzpolitik/bnd-affaere-oesterreichischer-abgeordneter-zeigt-telekom-und-bnd-an-a-1034297.html

[4] Georg Mascolo, "Codewort Eikonal - der Albtraum der Bundesregierung",*Sueddeutsche.de*, 4. October 2014, http://www.sueddeutsche.de/politik/geheimdienste-codewort-eikonal-der-albtraum-der-bundesregierung-1.2157432

As this statement will show, the United States has engaged in a long and heated reform debate and achieved significant progress with a long list of policy changes. None has solved the key problem for Europeans -- whether and how the NSA will substantially restrict surveillance on foreign citizens. The immediate answer is that they will not, although reforms have greatly improved transparency and elevated the standards of privacy and civil liberties afforded to non-US persons.[5] Nonetheless, the policy changes in Washington are significant not just as a matter of law. They are significant because they indicate a change in how the American public and the US government perceive the necessity and the legitimacy of surveillance. It is a starting point -- a clear baseline in a realm of law long shrouded in secrecy -- for a long engagement for a democratic society that seeks to modernize privacy and security policy in the digital age.

Consider this statement from President Barack Obama in December of 2013:

> *"I think part of what's been interesting about this whole exercise is recognizing that in a virtual world, some of these boundaries don't matter anymore. And just because we can do something doesn't mean we necessarily should, and the values that we've got as Americans are ones that we have to be willing to apply beyond our borders, I think, perhaps more systematically than we've done in the past."*[6]

At the center of President Obama's comment is the tension between what is legal (and technically possible) on the one hand -- and what is legitimate on the other. What is legal is not necessarily also legitimate. This why we often revisit debates about laws, particularly if they are controversial. Context, interpretation, and methods of implementation matter greatly in the determination of public legitimacy. The core of the debate over NSA practices is fundamentally about the circumstances in which surveillance is legitimate in a democracy. No serious proposal has been made in any country to make surveillance of all types illegal. Indeed, no serious proposal has been made to eliminate all forms of "bulk" surveillance. But many countries -- perhaps most notably the US and Germany above all others -- are debating what is legitimate. And in the best spirit of democracies, the goals is to modernize the law to match the judgement we reach.

This question of legitimacy should be the central lens through which this Committee views the actions of its own government as well as those of other nations. Legitimacy is about three things. First, it is trust that power will be applied transparently and with due process according to the law. Second, legitimacy is trust that power will be constrained by democratic principles. And third, legitimacy is about effective oversight and accountability over the application of power with clear and effective controls. Even in a post-Snowden world, most people in Europe and the US do not oppose digital surveillance for law enforcement and intelligence. What they seek are

---

[5] Hereafter, "US persons" is used as a term of US law to mean US citizens or lawful permanent residents. See, e.g. https://www.nsa.gov/about/faqs/oversight.shtml#oversight3

[6] Edward Moyer, "Obama: NSA programs could be 'redesigned' to prevent abuses", *cnet.com*, 20. December 2013, http://www.cnet.com/news/obama-nsa-programs-could-be-redesigned-to-prevent-abuses/

stronger guarantees that the application of state power is clear, limited, and properly controlled within and among nations.

I have been asked by the committee to provide an overview of the post-Snowden debate and reform efforts in the United States. A thorough documentation of arguments, counterarguments, studies, reports, and policy changes (proposed and enacted) could easily fill a book. And a great deal of this story would be about Americans arguing about how and whether the NSA is respecting their own privacy rights -- completely aside from the international issues that occupy this committee. After thinking carefully about the question what could be most relevant for the work of this committee, I have come to the conclusion that I should focus my statement on the issue that is most relevant to Germans. While the debate about the impact of surveillance programs on Americans is important and significant, Germans naturally care most about the implications of these programs on their own privacy.

This question goes directly to the heart of the problem of legitimacy. When it comes to the operation of its foreign intelligence agencies, every democratic country draws a strict line between citizens and people residing on its territory (in the US context referred to as US persons) and everyone else. From a German perspective this means that Germans enjoy certain rights and protections vis-a-vis surveillance undertaken by German government agencies. But Germans are pretty much fair game concerning surveillance undertaken by NSA, GCHQ or anyone else. While the Russian and the Chinese government may not care about this discrimination in rights to privacy (since they may not even afford them to their own citizens), it poses a legitimacy problem for any liberal democracy. As President Obama put it: "just because we *can* do something, doesn't necessarily mean we *should*." (emphasis added)

In the context of international relations and surveillance policy, the key question is how national laws governing intelligence collection will handle the privacy rights and civil liberties of foreigners -- the "discrimination problem." Addressing the discrimination problem will be a central element for any nation's development of a legal framework for foreign intelligence collection that is not only perceived as legitimate by its own citizens but also by this country's allies and partners. The discrimination problem has been clearly recognized as central to the debate in the United States. Not surprisingly, the human rights community has strongly criticized the lack of privacy protections afforded to non US-persons. They have argued this is in clear violation of human rights treaty obligations. The German and Brazilian governments joined to submit a resolution to the UN General Assembly calling attention to the human rights violations that may result from extraterritorial mass surveillance.[7]

Meanwhile, US technology and Internet companies have been vocal supporters of reforms to afford more protections to foreign citizens. These companies are not driven by altruism. As global players they are foremost concerned about the loss of market shares overseas. For

[7] Deutsche Welle, "Germany and Brazil circulate UN draft resolution on condemning surveillance", 2. November 2013, http://www.dw.com/en/germany-and-brazil-circulate-un-draft-resolution-on-condemning-surveillance/a-17199877

example, the CEO of Facebook, Mark Zuckerberg, reacted with outrage to the initial response from the US government regarding the Prism program.

> *The government response was, 'Oh don't worry, we're not spying on any Americans.' Oh, wonderful: that's really helpful to companies trying to serve people around the world, and that's really going to inspire confidence in American internet companies.*[8]

Two years into the debate, Silicon Valley has turned out to be a powerful ally for those who seek not only to improve the privacy rights of US citizens but of everyone around the globe. While these companies have not been successful in moving policy-makers to enact a common standard of privacy rights, they have achieved new authorization to increase their own levels of transparency about the nature and frequency of the data requests they get from law enforcement.

After a great deal of debate, review, and deliberation, the US government has enacted various reforms in the area of privacy rights for non-US persons. They have received little attention in the European media. But they do reflect a sustained effort to address the concerns of foreign governments and citizens, to increase transparency about the principles, circumstances and procedures of foreign intelligence collection, and to make concrete changes to law and practice. These efforts are far from sufficient to solve the discrimination problem. But they are an important starting point for future reforms. And I argue that any country that seeks to engage the US government on the discrimination problem will have to at least meet the threshold of these reforms. As I will point out in the conclusion, the work of this inquiry committee and the intensity and seriousness of the debate in Berlin have put Germany in a strong position to set a much higher standard. But as the US case shows, it will require serious work.

My concrete objective in this statement is to describe briefly the political debate over surveillance in the United States in the post-Snowden period and to evaluate the policy reforms that have been proposed or enacted -- specifically with relevance to the privacy rights and civil liberties of non-US persons. In the first section, I will offer a review of how US law is structured to oversee and guide the practice of signals intelligence collection. In the second section section, I will review the most important reform efforts initiated and/or completed by the Obama administration. Finally, in the third section, my purpose is to return to the themes of this introduction and suggest that the history of the reform debate in the US in the last two years should be read as a beginning and not an end. But as the work of this committee has shown, the surveillance problem will not and cannot be solved in Washington alone. The reforms enacted by the Obama administration set a new baseline of rights, standards, and transparency in the surveillance practices of democratic societies. It may fall well short of the desired expectations of America's European allies. But it is foundation to work from -- policies lifted out of the classified world of intelligence agencies and placed in public view for scrutiny and debate.

[8] Dominic Rushe, "Zuckerberg: US government 'blew it' on NSA surveillance", *TheGuardian.com*, 12. September 2013, http://www.theguardian.com/technology/2013/sep/11/yahoo-ceo-mayer-jail-nsa-surveillance

With its historical commitments to privacy and civil liberties, Germany can lead by example, presenting arguments for further reform and setting new standards of law and legitimacy which all other nations may join and against which all other nations will be judged.

Part 1: Overview of US Surveillance Law

The US legal framework that governs surveillance for intelligence purposes (as distinct from public policing and law enforcement) contains three basic elements -- authorization, operation, and oversight. The first set of rules governs the principles, standards and processes for authorizing a surveillance operation. The second set of rules apply to surveillance operations that have been authorized. They pertain to restrictions such as duration of surveillance, period of data storage, incidental collection, errors or false positives, and rules about the sharing of data with other agencies. Finally, the third set of rules establishes oversight practices within the intelligence agency, within the executive branch of government that controls the agency, and within the legislature elected to run the government. The scope and mandate of the oversight instruments determines whether it is sufficient to hold decision-makers accountable to the standards of authorization and operation.

In the US, foreign intelligence collection is governed in these three areas under various statutes and executive orders/directives that are applied in different ways depending on the target and nature of the surveillance. A full analysis of all variations of how particular laws govern particular types of surveillance operations is beyond the scope of this statement and unnecessary for its purposes. A short discussion of the three most common statutory bases will suffice to demonstrate the key points.[9]

Section 215 of the PATRIOT Act (2001)[10]: This statute was passed in the wake of the 9/11 terror attacks. This provision authorizes the collection of "tangible things" or "business records" to support an investigation with a foreign intelligence purpose -- e.g. counterterrorism. Most notably, this law was used to authorize the NSA's bulk collection of metadata from all phone calls made or received by residents of the United States. Under this statute, targets are non-US person about whom there are reasonable grounds to believe personal data records will contain foreign intelligence information relevant to an investigation. Section 215 orders may authorize a very broad collection of records. They are authorized by the Foreign Intelligence Surveillance Court (FISC). Operations conducted on this data set are restricted by usage and minimization practices. These are either standardized practices within the NSA or FBI -- or they are specified

[9] Report and Recommendations of The President's Review Group on Intelligence and Communications Technologies, "Liberty and Security in a Changing World", 12. December 2013, https://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf (see Appendix A) ; Ian Brown et al., "Towards Multilateral Standards for Surveillance Reform", http://voxpol.eu/wp-content/uploads/2015/01/HERE.pdf

[10] H.R. 3162, "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001", http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=107_cong_bills&docid=f:h3162enr.txt.pdf

by the FISC.[11] Oversight of Section 215 programs is conducted by the operating agencies themselves, the Director of National Intelligence, the Department of Justice, as well as the Privacy and Civil Liberties Oversight Board and the Congressional intelligence committees.

Foreign Intelligence Surveillance Act (1978)[12]: FISA was enacted after the Watergate scandals of the Nixon era in which federal agencies were used to spy on American citizens. FISA established new rules to govern and oversee surveillance activities for the purposes of foreign intelligence collection, explicitly distinguishing between the standards applied to US persons and non-US persons. FISA established the Foreign Intelligence Surveillance Court (FISC) to review classified requests by agencies to conduct surveillance operations for particular purposes, e.g. counter-terrorism.

FISA has been amended many times over the years, and most importantly by the 2008 FISA Amendments Act (FAA). The FAA established a new provision -- Section 702 -- which specifically authorizes foreign surveillance operations targeting non-US persons outside the United States for the collection of telecommunications data (phone and email content included) by the NSA. The Attorney General and the Director of National Intelligence may determine targets of non-US person for periods of up to one year. Specific judicial review for particular targets was not required, if the target is subject to one of the broad certifications for foreign intelligence collection authorized by the FISC. These annual authorizations must be approved by the FISC, and they are drawn from the (classified) National Intelligence Priorities Framework. The lengthy guidelines for restrictions on Section 702 operations (minimization practices) have been declassified and published.[13] These include specific instructions for how data should be handled, stored, queried, and processed. Oversight of Section 702 operations is conducted by the NSA itself, the DNI, and the congressional oversight committees.

Section 702 of the Foreign Intelligence Surveillance Act authorizes two prominent bulk collection programs revealed by the Snowden files: PRISM and UPSTREAM.[14] The PRISM program requires participating US Internet companies to hand over communications related to selectors (email address, account name, etc.) which they receive from a security agency. The UPSTREAM program is much broader in scope. Here the NSA utilizes Section 702 authority to gain direct access the networks of telecommunications companies at an Internet Exchange Point or similar network interconnection points. The entire data stream is searched and

[11] See for example the detailed minimization requirements for the telephone metadata program described in this declassified FISC decision: http://www.dni.gov/files/documents/PrimaryOrder_Collection_215.pdf
[12] Public Law 95-511, “Foreign Intelligence Surveillance Act of 1978”, http://www.gpo.gov/fdsys/pkg/STATUTE-92/pdf/STATUTE-92-Pg1783.pdf
[13] U.S. Foreign Intelligence Surveillance Court, “Minimization Procedures used by NSA in Connection with FISA Section 702”, 31. October 2011, https://www.aclu.org/sites/default/files/field_document/minimization_procedures_used_by_nsa_in_connection_with_fisa_sect_702.pdf
[14] Privacy and Civil Liberties Oversight Board, “Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act”, 2. July 2014, https://www.pclob.gov/library/702-Report.pdf

analyzed with selectors, and then relevant communications (including phone calls) are stored in large data bases for subsequent processing.

Executive Order 12333 (1981)[15]: This executive order outlines the rules governing conduct of foreign intelligence collection across all agencies. It does not supercede the provisions of FISA but it covers all activities not addressed by FISA.[16] EO 12333 (amended three times over the years -- including in 2008) authorizes foreign intelligence collection outside the US and identifies principles and priorities. The minimization procedures designed to restrict targeting of US persons remain classified. Oversight is conducted by the relevant agencies, the National Security Council, and the DNI.

The vast majority of the NSA's foreign surveillance programs[17] is conducted under the authorization of EO 12333. An official 2007 surveillance manual states that EO 12333 "is the primary source of NSA's foreign intelligence-gathering authority."[18] Since the executive branch issues and implements the order, there is very little oversight from Congress or courts. One program that is known to be authorized by EO 12333 is MUSCULAR - a joint project between GCHQ and NSA. The goal is to tap into the worldwide fiber optic networks that connect the data centers of Google, Yahoo and others.[19]

The legal framework for foreign intelligence collection is very extensive and complex. Secrecy regarding the interpretation of statutory authority by the NSA and other intelligence agencies, the classification of FISC rulings, and the lack of public information regarding Executive Order 12333 make a thorough assessment very difficult. But there is no doubt that the framework is premised on much weaker standards for authorization, operational practice, and oversight in regard to the surveillance of foreigners than the legal standards applying to the surveillance of US persons. That division is axiomatic for laws governing the targets of *foreign* intelligence collection, but it also reflects the constitutional rights afforded only to citizens and the separate legal procedures with much higher standards of protection for privacy and civil liberties required for investigations of US persons.

Part 2: US Debate and Reform Efforts

---

[15] Executive Order 12333 - United States Intelligence Activities, http://www.dni.gov/index.php/about/organization/ic-legal-reference-book-2012/ref-book-eo-12333; Scott F. Mann, "Fact Sheet: Executive Order 12333", *Center for Strategic & International Studies*, 24. February 2014, http://csis.org/publication/fact-sheet-executive-order-12333-0

[16] *McClatchyDC*, "Most of NSA's data collection authorized by order Ronald Reagan issued", 21. November 2013, http://www.mcclatchydc.com/news/nation-world/national/national-security/article24759289.html

[17] ProPublica, "The NSA Revelations all in one chart", https://projects.propublica.org/nsa-grid/

[18] DOCID 4145825, Overview of Signals Intelligence Authorities, https://www.aclu.org/files/assets/eo12333/NSA/Overview%20of%20Signals%20Intelligence%20Authorities.pdf

[19] Kim Zetter, "Report: NSA Is Intercepting Traffic From Yahoo, Google Data Centers", 30. October 2013, http://www.wired.com/2013/10/nsa-hacked-yahoo-google-cables/

The debate over surveillance policy in the United States after the Snowden disclosures was widespread and high profile. Voices calling for reform ranged across the political spectrum -- including left-leaning Democrats and the Republican authors of the PATRIOT Act. Dozens of Silicon Valley companies and civil liberties NGOs responded first in July 2013 with a letter to government leaders calling for more transparency in surveillance programs.[20] In December 2013, a group of the most prominent American technology companies formed a new corporate coalition -- known as Reform Government Surveillance -- proposing an end to mass surveillance and proposing a set of reforms to oversight, transparency, and operational practice.[21] In January 2014, a group of prominent cryptographers and a much larger group of scholars joined letters calling for an end to mass surveillance.[22] A coalition of civil society organizations -- focused on civil liberties, human rights, and Internet freedom -- formed to push for change that numbered dozens of groups representing millions of people.

The grassroots campaign called on Congress to change the law to curb surveillance. On a single day -- February 11, 2014 -- the campaign reached 37 million people, generating more than half a million messages to Congress, tens of thousands of phone calls to elected officials, and hundreds of thousands of signatures on petitions.[23] These groups have remained well organized and made consistent calls for legislative change, marshalled sophisticated legal analysis, and lobbied Congress.[24] The corporate and civil society coalitions joined forces to push for passage of the USA Freedom Act and continue to deliver broad bipartisan support for their cause.

Since June 2013, more than 25 court cases against US government surveillance programs have been filed.[25] NGOs like the American Civil Liberties Union or the Electronic Frontier Foundation have challenged the legality of different programs and the US government's interpretation of central legal frameworks such as the PATRIOT Act or the Foreign Intelligence Surveillance Act. In addition, companies like Google and Yahoo successfully went to court to win the right to reveal more information about requests for user data in their transparency reports.[26]

Although one of the most prominent lawsuits -- ACLU v. Clapper[27] -- focuses solely on the domestic phone record program, there have been other lawsuits with implications for the privacy

[20] The New York Times, "Silicon Valley Letter Calling for Surveillance Disclosure", http://www.nytimes.com/interactive/2013/07/18/us/18nsa-letter.html?_r=0
[21] At the time of writing the group consists of AOL, Apple, Dropbox, Evernote, Google, Microsoft and Yahoo: https://www.reformgovernmentsurveillance.com/
[22] April Glaser, "Academics and Researchers Against Mass Surveillance", *Electronic Frontier Foundation*, 12. February 2014, https://www.eff.org/deeplinks/2014/02/academics-and-researchers-against-mass-surveillance
[23] The Day We Fought Back, https://thedaywefightback.org/the-results/
[24] NSA coalition letter, https://www.eff.org/files/2015/03/24/nsa_coalition_letter_032515.pdf
[25] ProPublica, "NSA Surveillance Lawsuit Tracker", https://projects.propublica.org/graphics/surveillance-suits
[26] Center for Democracy and Technology, "Yahoo vs. US PRISM Documents", https://cdt.org/insight/yahoo-v-u-s-prism-documents/
[27] American Civil LIberties Union, "ACLU v. Clapper - Challenge to NSA Mass Call-Tracking Program", 3. September 2014, https://www.aclu.org/cases/aclu-v-clapper-challenge-nsa-mass-call-tracking-program

rights of foreigners. For example, the Wikimedia Foundation challenged the legality of the NSA's UPSTREAM program -- authorized by Section 702 of the Foreign Intelligence Surveillance Act.[28] While the number of court cases is impressive, most of them have not been heard yet or are still in process in the lower courts. As these cases make their way through the legal system, courts could take on an important role in pushing the US government to enact further reforms. However, US courts are unlikely to address the discrimination problem head on as they tend to focus on the scope of statutory authority and the protection of constitutional rights of US citizens.

By any standard, the level of organized calls for reform of surveillance policy in the US is impressive. However, much of this energy was focused on restricting the ways in which NSA intercepts and collects (directly or incidentally) the data of Americans. And while many of the protagonists in the reform coalitions would extend their support to the privacy rights of foreign citizens, the major themes in the American policy debate have been about American privacy rights. An important exception to this domestic focus are the views of American technology and telecommunications companies that operate in foreign markets. The compulsion under US law to hand over data of foreign customers presents them with a difficult dilemma. To comply with US law, they must violate the laws of foreign countries and the trust of foreign customers. For this reason, the economic dimension of the surveillance debate plays a significant role in driving a reform agenda focused internationally.

The response of the Obama administration to this public pressure for reform has been multi-faceted and unusually rapid by the standards of American policy change. Of course, none of the changes to policy and practice represents an "end to bulk surveillance" or resolved the discrimination problem in ways that satisfy the concerns of foreign nationals. But the collective result of the reforms (particularly in the area of transparency) is the most significant change in modern American intelligence gathering in decades.[29] The political pendulum swing towards maximizing security that began after 9/11 has begun to swing back towards civil liberties. This is not just about change of law -- although some significant surveillance programs have been found unlawful by the courts. The majority of the changes were not necessary to be legal. They were done to foster and promote legitimacy.

For ease of review, the reforms enacted by the Obama administration are grouped into three categories: 1) analysis, review, and investigation of signals intelligence programs by independent panels of experts; 2) changes to oversight, transparency and compliance; and 3) broader changes to law and policy.

---

[28] Michelle Paulson and Geoff Brigham, "Wikimedia v. NSA: Wikimedia Foundation files suit against NSA to challenge upstream mass surveillance", Wikimedia blog, 10. MArch 2015, http://blog.wikimedia.org/2015/03/10/wikimedia-v-nsa/

[29] Timothy H. Edgar, "The Good News about Spying", *Foreign Affairs*, 13. April 2015, https://www.foreignaffairs.com/articles/united-states/2015-04-13/good-news-about-spying ; Peter Swire, "The USA FREEDOM Act, the President's Review Group and the Biggest Intelligence Reform in 40 Years", *The International Association of Privacy Professionals*, 8. June 2015, https://privacyassociation.org/news/a/the-usa-freedom-act-the-presidents-review-group-and-the-biggest-intelligence-reform-in-40-years

Review & Investigation

The Snowden disclosures and consequent political debate triggered the formation and empowerment of a number of special review groups, oversight investigations, and scholarly studies of US intelligence practices. Many were undertaken by the federal government and a host of others were sponsored by private companies, academic institutions, and NGOs. A full review of these analyses is beyond the scope of this paper. However, I will highlight three of the most important government-sponsored oversight efforts. Each produced extensive reports that highlighted the existing problems with intelligence policy and practice. And each offered clear recommendations for reform. Many of the key recommendations are directly relevant to the question of privacy and security rights for non-US persons.

President's Review Group on Intelligence and Communications Technologies[30]: In mid-August after the initial Snowden revelations in June of 2013, the White House established a special Review Group to evaluate intelligence collection practices using communications technologies with a focus on evaluating the best methods of protecting both privacy and security interests.[31] Among the key questions analyzed by the review group were several relevant to the privacy rights of non-US persons -- including the procedures for restricting collection, processing and sharing of foreign intelligence data and the treatment of unbreakable encryption standards in the international marketplace.

The five members of the review group were all former senior government officials or academic experts with strong expertise, experience and credibility on these topics. The work of the Review Group was conducted very rapidly (the final report was published in December 2013) and its scope was very broad. Critics argued that this group (which included a former CIA deputy director and a former White House counterterrorism advisor) represented an "insider" view of security policy that would inevitably tilt their views to favor the intelligence community. However, the final report delivered 46 detailed recommendations for reform -- many of them quite critical and proposing expansive changes to intelligence gathering practices. The implications of this group calling for such extensive reforms were praised by reformers.[32] It remains the most comprehensive blueprint for modernization of security and privacy policy written by any oversight body.

---

[30] Report and Recommendations of The President's Review Group on Intelligence and Communications Technologies, "Liberty and Security in a Changing World", 12. December 2013, https://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf

[31] Office of the Director of National Intelligence, "The Review Group", http://www.dni.gov/index.php/intelligence-community/review-group

[32] Ellen Nakashima and Ashkan Soltani, "NSA shouldn't keep phone database, review board recommends", *The Washington Post*, 18. December 2013, https://www.washingtonpost.com/world/national-security/nsa-shouldnt-keep-phone-database-review-board-recommends/2013/12/18/f44fe7c0-67fd-11e3-a0b9-249bbb34602c_story.html

Most of the Review Group's recommendations have not been implemented. But those that have include serious changes to intelligence practices -- such as an end to the NSA's bulk collection of telephone metadata records (see below -- USA Freedom Act). The recommendations for greater transparency and limits on bulk collection (including foreign sources) have also been realized (at least in part) through the publication of intelligence collection standards, minimization practices, and the decisions of the FISC.[33] Other important reform proposals -- that have not been implemented -- in the report include a call to support strong encryption (without mandatory back-doors) and a recommendation to negotiate arrangements among allied nations to apply greater restraint to the surveillance of foreign leaders.

The Privacy and Civil Liberties Oversight Board Reports.[34] The Privacy and Civil Liberties Oversight Board (PCLOB) was established in 2007 as a part of the laws implementing the recommendations of the 9/11 Commission. It is an independent and bipartisan agency charged with reviewing the counterterrorism activities of the US government to ensure the appropriate protection of privacy and civil liberties. After the Snowden disclosures, the PCLOB conducted an ongoing series of multi-stakeholder expert hearings and undertook the analysis of the major statutes authorizing signals intelligence collection -- including Section 215 of the PATRIOT Act and Section 702 of the FISA.[35] The resulting findings presented in two major reports played an influential role in shaping public perception and the reform proposals introduced by policymakers in the White House and the US Congress. Notably, the PCLOB report on Section 215 recommended an end to the program -- foreshadowing the legislative solution later passed in the USA Freedom Act. The PCLOB report criticized the legal justification of the bulk collection program (later validated by a federal court), highlighted the danger the program posed to privacy rights, and joined the White House Review Group's conclusion that the program appears to have limited utility. The PCLOB investigation and study of Section 215 surveillance could not identify a single instance in which the bulk collection program was a critical factor in a counterterrorism operation. Much of the media attention surrounding the PCLOB reports focuses on the Board's conclusions about how the privacy rights of US persons should be protected. But the reports are quite relevant to the broader question of privacy rights within foreign intelligence collection as well.

The PCLOB reports on Section 215[36] and Section 702[37] were published in January and July of 2014 respectively. They included more than 20 recommendations for reform directed at the Executive Branch, the Intelligence Community, the FISA Court, and the US Congress. Many have now been implemented or are in the process of being implemented. The PCLOB published an assessment of the response of the federal government to its recommendations in January of

[33] See footnote 28
[34] PCLOB, Document Library - Oversight Reports, https://www.pclob.gov/library.html#oversightreports
[35] An analysis of Executive Order 12333 is currently in progress.
[36] PCLOB,"Report on the Telephone Records Program Conducted under Section 215 of the USA PATRIOT Act and on the Operations of the Foreign Intelligence Surveillance Court", 23. January 2014, https://www.pclob.gov/library/215-Report_on_the_Telephone_Records_Program.pdf
[37] PCLOB,"Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act", 2. July 2014, https://www.pclob.gov/library/702-Report.pdf

2015.[38] Highlights include a number of issues that were also addressed by the Review Group as well as the USA Freedom Act. For example, the PCLOB recommended that the FISC hear from independent legal and technical experts (including a Special Advocate for privacy and civil liberties) when reviewing bulk collection programs. The PCLOB recommended the government publish FISC orders that decide novel questions of law and submit its decisions to appellate review. This recommendation joined a number of others regarding increased transparency in how companies are queried for data records through these programs.

More directly relevant to the privacy of non-US persons, the PCLOB recommended changes in the way that the NSA evaluates foreign surveillance targets under Section 702. The PCLOB report found that the targeting procedures are rigorous in their determination about whether the target is a non-US person outside the US. But the standard for evaluating whether there is a legitimate foreign intelligence purpose for the target was much lower. The administration agreed to raise the standard in accordance with the PCLOB recommendation. The administration also agreed with another PCLOB recommendation to submit to the FISC a random sample of tasking sheets featuring targeting information along with the overall request for certification of broader foreign intelligence purposes. This spot checking will permit more careful review of actual practice and selectors rather than limiting judicial review to higher level issues. Finally, the PCLOB secured agreement from the Intelligence Community to prepare for the publication of declassified versions of minimization procedures used by the agencies to avoid collecting and processing communications from unauthorized targets.

National Research Council Report. Among the recommendations[39] of the White House Review Group was a proposal to conduct a technical analysis of how software could be designed to limit the use of bulk collection methods in signals intelligence in favor of targeted surveillance. This recommendation was turned into action by Presidential Policy Directive 28 (January 2014). The result was a study published by the National Research Council (a part of the National Academy of Sciences) in January 2015 entitled -- *Bulk Collection of Signals Intelligence: Technical Options*.[40] The report is relevant to the privacy of foreign intelligence targets because it directly evaluates the necessity of bulk collection (which incidentally sweeps in the communications of unauthorized targets) and analyzes the technical options to limit the potential for infringing on the rights of unauthorized targets. The report has three major conclusions.[41] First, the NRC argues that bulk collection is unavoidable, if the purpose of the collection is to create a reservoir of data to evaluate later as relevant foreign intelligence targets become known (e.g. looking back at the collected communications of individuals later identified as potential terrorists). There is considerable debate about the utility of this "intelligence time machine" theory of signals intelligence that collects haystacks of data in order to search for

[38] PCLOB, "Recommendations Assessment Report", 29. January 2015, https://www.pclob.gov/library/Recommendations_Assessment-Report.pdf
[39] See Op Cit., footnote 30 (page 33, Recommendation 20).
[40] National Research Council, "Bulk Collection of Signals Intelligence: Technical Options", 15. January 2015, http://www.nap.edu/openbook.php?record_id=19414
[41] Andy Wang, "The NRC's Bulk Collection Report: a High-Level Overview", *Lawfare*, 20. January 2015, http://www.lawfareblog.com/nrcs-bulk-collection-report-high-level-overview

needles sometime in the future.[42] But the NRC report concludes there is no technical alternative. Second, the report argues that despite concluding that bulk collection cannot be avoided by software that enables a more targeted approach, technology could improve the privacy restrictions placed on a particular surveillance operation. Restrictions on queries, access, combination of data, and dissemination can be hard-coded into the software to deter violations that may occur through human error or intentional abuse. And finally, the report concludes that further development of software could improve the filtering technologies that automatically delete data that is not relevant to the search terms and thus de facto create a more targeted approach to bulk collection.

Oversight, Transparency and Compliance

In part in response to the analysis and recommendations in the Review Group and PCLOB reports, the US Intelligence Community (IC) has begun an unprecedented process to offer the public more transparency into its operations -- including on issues directly and indirectly related to the privacy rights of non-US persons. On a new website called “IC on the Record”, the agencies have published a wide variety of documents and explanations related to statutory authorization, operational practice, minimization procedures, and oversight methods. A significant part of the content is driven by orders in Presidential Policy Directive 28 (see below) for the IC to revise policies and procedures to elevate privacy protections and safeguard personal information. In addition, the intelligence community has adopted a number of specific reforms to operational procedures -- including several related to oversight, training, and transparency. Finally, it is noteworthy that the National Institute of Standards and Technology (NIST) -- a unit of the Department of Commerce called out by security professionals for endorsing a cryptographic standard considered to be compromised by the NSA[43] -- has changed its recommendations on cryptography to remove doubt from the integrity of its work.[44]

IC on the Record[45]: The tumblr site maintained by the Office of the Director of National Intelligence was created at the direction of the President. Its design is to publish factual information about foreign intelligence collection activities to increase transparency. It contains declassified documents, official statements, congressional testimony of senior leadership, speeches, fact sheets, and the new annual report documenting the steps being taken by the IC to reform its practices to better protect privacy and civil liberties. Among the notable content available on the site are several issues with relevance to the privacy rights of non-US persons. These include:

---

[42] Marshall Erwin, “The Intelligence Time Machine”, *JustSecurity*, 30. April 2015, http://justsecurity.org/22560/intelligence-time-machine/

[43] Michael Mimoso, “In Wake of Latest Crypto Revelations, ‘Everything is Suspect’”, *ThreatPost*, 20. September 2013, https://threatpost.com/in-wake-of-latest-crypto-revelations-everything-is-suspect/102377

[44] Dennis Fisher, “NIST Drops Weak Dual_EC RNG From Official Recommendations”, *ThreatPost*, 26. June 2015, https://threatpost.com/nist-drops-weak-dual_ec-rng-from-official-recommendations/113493

[45] Office of the Director of National Intelligence - IC on the Record, http://icontherecord.tumblr.com/

- *IC Transparency Reports*.[46] The IC has begun publishing annual transparency reports that present data such as the number of FISA orders granted in a particular year and the number of targets affected. These raw numbers are not particularly insightful because they do not specify the number of non-US persons affected by particular orders or targeting lists. Nonetheless, it is an unprecedented level of transparency for any foreign intelligence operation.

- *NSA's Supplemental Privacy Procedures.*[47] All agencies in the IC have (as required by PPD 28) produced new guidelines to update and improve procedures to safeguard personal information -- including specifically the personal information of non-US persons. These supplemental guidelines propose to treat the privacy of non-US persons in comparable ways to US persons in so far as that is "consistent with national security." These procedures appear to be a straightforward statement of compliance with existing law. However, the publication of such procedures is itself a noteworthy degree of transparency. The substantive changes reflect the requirements of Presidential directive, including the provision that non-US persons data will be deleted after 5 years (unless specifically exempted by the ODNI, or if it is encrypted). Previously, the length of data retention varied across the IC -- now it is standardized at 5 years, with these exceptions. This limitation is considered by some security analysts as a significant new restriction.[48]

- *Declassified Operational Documents.*[49] The IC has declassified and published a number of informative documents regarding how they work. These include -- for example -- the NSA[50] and CIA[51] minimization procedures for deleting, processing, sharing, and retaining data collected from foreign nationals under Section 702 of FISA.

- *Declassified FISC decisions.* In response to a PCLOB recommendation, the IC has begun declassifying and publishing past FISC opinions that deal with novel questions of law or technology. In addition, they purport to be in the process of declassifying current decisions that deal with novel question of law or technology.[52]

---

[46] IC on the Record, "Calendar Year 2014 Transparency Report", 22. April 2015, http://icontherecord.tumblr.com/transparency/odni_transparencyreport_cy2014
[47] National Security Agency, "PPD-28 Section 4 Procedures", 12. January 2015, https://www.nsa.gov/public_info/_files/nsacss_policies/PPD-28.pdf
[48] Carrie Cordero, "First Take on Government's Surveillance Reform Update Report", *Lawfare*, 4. February 2015, http://www.lawfareblog.com/first-take-governments-surveillance-reform-update-report
[49] IC on the Record, "Release of Documents Concerning Activities under the Foreign Intelligence Surveillance Act", 3. March 2015, http://icontherecord.tumblr.com/post/112610953998/release-of-documents-concerning-activities-under
[50] Foreign Intelligence Surveillance Court, "Standard Minimization Procedures for Electronic Surveillance Conducted by the National Security Agency (NSA)", 13. December 2006, http://www.dni.gov/files/documents/0315/NSA%20Minimization%20Procedures.pdf
[51] Foreign Intelligence Surveillance Court, "CIA Minimization Procedures for Information from FISA Electronic Surveillance conducted by NSA", 13. December 2006, http://www.dni.gov/files/documents/0315/CIA%20Minimization%20Procedures.pdf
[52] See footnote 39 (pages 9-10).

Procedural and Operational Changes. In addition to increasing transparency, the IC has made a set of changes to how they operate that are worthy of note because several of them directly affect the protection of personal information for non-US persons.[53]

- *Limits on Section 702 Collection.* In response to the PCLOB report on Section 702, the ODNI has ordered changes to procedures. These include revising the process to require additional documentation from the analyst that the target is not only a non-US person outside the US but also that the target's communications hold foreign intelligence value (previously, the latter documentation was not required). It also includes the restriction on retaining data for more than 5 years without specific authorization from the ODNI.[54]

- *Increase White House Oversight of Sensitive Collection.* The White House has announced in PPD 28 that it will actively intervene to avoid unilateral targeting decisions by the IC on sensitive intelligence collection. In particular economic and diplomatic decision-makers in government will be consulted on these choices. Sensitive topics include surveillance of foreign leaders.

- *Funding Increases for PCLOB and MLAT Processing*. Budget requests from the administration and spending bills before Congress would significantly increase the funding for the PCLOB's activities[55] as well as the processing of Mutual Legal Assistance Treaty requests by the Department of Justice.[56] (MLATS are the agreements that enable cross-border criminal investigation including data requests.) These are important institutional reforms to ensure that the oversight and attention to safeguarding the privacy of non-US persons remains relevant and sustained.

NIST Standards on Cryptography. In addition to the changes happening within the IC, there are related institutional reforms. For example, the National Institute for Standards and Technology has removed a standard for the generation of random numbers from its official recommendations.[57] This standard had previously come under sharp criticism by cryptography experts as too weak to guarantee security and perhaps intentionally compromised by

---

[53] Peter Swire, "Preparing to Debate NSA Surveillance and Online Commercial Tracking", *The International Association of Privacy Professionals*, 18. February 2015, https://privacyassociation.org/news/a/preparing-to-debate-on-nsa-surveillance-and-online-commercial-tracking/

[54] Alex Ely, "DNI Report on Implementation of Signals Intelligence Reforms: Some Highlights", *Lawfare*, 8. February 2015, http://www.lawfareblog.com/dni-report-implementation-signals-intelligence-reforms-some-highlights

[55] Julian Hatten, "Spending bill more than doubles money for privacy watchdog", *The Hill*, 9. December 2014, http://thehill.com/policy/technology/226574-spending-bill-more-than-doubles-money-for-privacy-watchdog

[56] US Department of Justice, "Mutual Legal Assistance Treaty Process Reform", *FY 2015 Budget Request*, http://www.justice.gov/sites/default/files/jmd/legacy/2014/07/13/mut-legal-assist.pdf

[57] The National Institute of Standards and Technology (NIST), "NIST Revises Key Computer Security Publication on Random Number Generation", 25. June 2015, http://www.nist.gov/itl/csd/random-number-generation.cfm

participation of the NSA in the standard setting working groups.[58] A recent amendment to a House spending bill would actively prohibit NIST from consulting with NSA or CIA on its cryptographic standards work.[59]

New Policy

Presidential Policy Directive 28[60]. The most significant change in federal policy with respect to foreign intelligence collection and the privacy standards applied to non-US persons was enacted by PPD 28. Announced in a major speech by President Obama[61] that addressed the controversy over NSA, privacy, and security policy, PPD 28 lays out a reformed set of guidelines and requirements for signals intelligence collection by US agencies.[62] It is the only document of its kind from any nation that is public.[63] The speech is essentially a defense of the IC's practices as legal and consistent with American values. But it acknowledges the need for modernization and a recalibration of practices and policies to restore trust in the credibility of privacy protections -- not just for Americans, but for all people of the world. PPD 28 is a policy change designed not to make major changes in law to programs deemed unlawful -- but rather a policy designed to reestablish legitimacy through transparency, oversight, and raising standards to safeguard personal information and restrict the use of powerful signals intelligence tools to very specific purposes.

The major provisions of PPD 28 with respect to privacy protections for foreign nationals are these -- many of which were already law but now have been stated in a single document in clear terms:

Purpose Limitations. PPD 28 sets out the exclusive purposes for which bulk collection of signals intelligence may be permitted.

---

[58] Mike Masnick, "NSA & GCHQ Covertly Took Over Security Standards, Recruited Telco Employees To Insert Backdoors", *techdirt*, 5. September 2013, https://www.techdirt.com/articles/20130905/12295324417/nsa-gchq-covertly-took-over-security-standards-recruited-telco-employees-to-insert-backdoors.shtml

[59] Amendment to H.R. 2578, offered by Mr. Massie of Kentucky, 3. June 2015, http://repcloakroom.house.gov/uploadedfiles/cjs16massie4.pdf

[60] The White House - Office of the Press Secretary, "Presidential Policy Directive -- Signals Intelligence Activities", 17. January 2014, https://www.whitehouse.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities

[61] The White House - Office of the Press Secretary, "Remarks by the President on Review of Signals Intelligence", 17. January 2014, https://www.whitehouse.gov/the-press-office/2014/01/17/remarks-president-review-signals-intelligence

[62] Mark Landler and Charlie Savage, "Obama Outlines Calibrated Curbs on Phone Spying", *The New York Times*, 17. January 2014, http://www.nytimes.com/2014/01/18/us/politics/obama-nsa.html?_r=1

[63] Benjamin Wittes, "The President's Speech and PPD-28: A Guide for the Perplexed", *Lawfare*, 20. January 2014, http://www.lawfareblog.com/presidents-speech-and-ppd-28-guide-perplexed

> *(1) espionage and other threats and activities directed by foreign powers or their intelligence services against the United States and its interests; (2) threats to the United States and its interests from terrorism; (3) threats to the United States and its interests from the development, possession, proliferation, or use of weapons of mass destruction; (4) cybersecurity threats; (5) threats to U.S. or allied Armed Forces or other U.S or allied personnel; and (6) transnational criminal threats, including illicit finance and sanctions evasion related to the other purposes named in this section.*

Privacy and Civil Liberties Principles. PPD 28 prohibits the collection of foreign intelligence for the purpose of suppressing political dissent or "disadvantaging persons based on their ethnicity, race, gender, sexual orientation or religion." These principles are universally applied.

> *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. U.S. signals intelligence activities must, therefore, include appropriate safeguards for the personal information of all individuals, regardless of the nationality of the individual to whom the information pertains or where that individual resides.*

Prohibits Industrial Espionage. PPD 28 explicitly prohibits the collection and dissemination of intelligence for the purposes of giving commercial advantage to US business interests.

Safeguards and Procedures for Privacy Protection. Section 4 of PPD 28 directs the IC to review and update its privacy standards and safeguards applying -- "to the maximum extent feasible consistent with national security" -- to all people regardless of nationality. This includes a minimization standard to restrict the retention of personal data to 5 years and to restrict the dissemination of personal data to the same standard for comparable information of a US person (which, notably, is not a particularly strict standard)[64]. Personal data must be stored under secure conditions to prevent unauthorized access, and personal data will only be used in intelligence reporting when that data has specific foreign intelligence value. Finally, the section requires a renewed emphasis on oversight and orders a series of reports on the implementation of these policies by the IC in the subsequent months.

Coordinator for International Diplomacy. PPD 28 also orders the Secretary of State to designate a senior official to serve as the interface with all foreign governments that wish to raise concerns about the US policies of signals intelligence.[65]

PPD 28 is an extraordinary document despite making relatively few significant changes to policy and practice. It applies common principles of privacy and civil liberties to intelligence collection regardless of nationality. It places specific purpose limitations on the bulk collection of signals intelligence. And it establishes procedures and standards to safeguard the privacy of non-US

[64] Executive Order 12333 - United States intelligence activities, 2.3 Collection of Information, http://www.archives.gov/federal-register/codification/executive-order/12333.html#2.3

[65] This role has been applied to the Undersecretary for Economic Growth, Energy and the Environment.

persons at the same level as US persons subject to national security interests. It is a baseline document that seeks to set standards for legitimacy under the law. All future reforms will be compared to this baseline. They will be judged against it; and they will build upon it.

USA Freedom Act (2015)[66]. One of the very first stories written about the classified documents disclosed by Edwards Snowden focused on a bulk collection program that permitted the NSA to collect, store, and query ALL metadata for all telephone calls in the US. The ostensible purpose was to ensure the interception of calls to and from non-US persons outside the US that have foreign intelligence value. The authority for this bulk collection program came from Section 215 of the PATRIOT Act -- a statutory provision that may be used to compel private companies to deliver business records or "tangible things." The scope of the NSA's reading of the law was authorized by a controversial FISC decision.

The legality of program (on both statutory and constitutional grounds) was quickly challenged in the courts. And ultimately -- almost two years later -- a federal appeals court ruled the program as authorized by the FISC was not a lawful reading of Section 215.[67] (This court case also raised the novel prospect of how previously classified FISC decisions may be treated for review in the normal course of appellate litigation.) Prior to the court decisions, both the White House Review Group and the PCLOB reviewed the Section 215 program and recommended its termination or at least major revisions to its operation that no longer authorized NSA collection and storage of bulk metadata records. The objections to the program in the political debate were largely focused on the vast collection of metadata records belonging to US persons (in pursuit of non-US person communications). However, major reform to the Section 215 metadata program would also have a beneficial impact on the privacy rights of non-US persons whose records were swept up in the bulk collection despite the absence of a foreign intelligence purpose.

In the spring of 2015, after several false starts, Congress ended this debate by passing the USA Freedom Act -- a bipartisan bill that enjoyed the support of the White House, the technology industry, and many civil liberties organizations. It is the first significant restriction of intelligence collection practices passed by Congress in more than 30 years. This legislation not only fundamentally changed the metadata collection program, it initiated a number of other key reforms to intelligence practice. The following provisions of the USA Freedom Act are directly or indirectly relevant to the privacy and civil liberties of non-US persons[68]:

---

[66] H.R. 2048 - USA FREEDOM Act of 2015, 2. June 2015, https://www.congress.gov/bill/114th-congress/house-bill/2048/text

[67] Charlie Savage and Jonathan Weisman, "N.S.A. Collection of Bulk Call Data Is Ruled Illegal", *The New York Times*, 7. May 2015, http://www.nytimes.com/2015/05/08/us/nsa-phone-records-collection-ruled-illegal-by-appeals-court.html;
US Court of Appeals for the Second Circuit, "ACLU v. Clapper", 7. May 2015, http://www.ca2.uscourts.gov/decisions/isysquery/5b758b27-c77d-44a2-b6e5-dbf456f5c142/1/doc/14-42_complete_opn.pdf

[68] US House of Representatives - Judiciary Committee, "USA Freedom Act", 3. June 2015, http://judiciary.house.gov/index.cfm/usa-freedom-act

- ➢ Prohibition on the collection of *all* metadata records as well as limitation that any bulk collection search terms submitted for authorization must not be indiscriminate (such as all records from a particular city). Metadata records will be retained by telecommunications companies (not the agency) and queried by security agencies only after judicial review of individual cases.[69]

- ➢ Permits companies to challenge "gag orders" that prohibit them from violating nondisclosure requirements attached to National Security Letters issued to compel communications data. Technology companies will also be permitted greater transparency with respect to publishing the number and nature of requests for data.

- ➢ Creates a panel of experts on privacy, civil liberties, and technology to offer consultation and guidance to the FISA Court.

- ➢ Requires the declassification of FISA Court opinions that contain novel interpretations of law, including the defined scope of search terms.

The USA Freedom Act codifies into law many of the recommendations initially presented in the White House Review Group report and the PCLOB review of the Section 215 programs. These include the elimination of bulk metadata collection stored by the government, a heightened standard of judicial review, limits on National Security Letters, increasing transparency in the FISC, and providing the court with expert and adversarial perspectives from technologists and civil liberties advocates.[70]

Judicial Redress Act (2015).[71] In the summer of 2014, then-Attorney General Eric Holder announced that the Obama administration would work with Congress to pass legislation granting EU citizens the right to seek redress in US courts under the provisions of the Privacy Act of 1974 in the same manner as US citizens.[72] This right would permit a path to legal remedy for EU citizens, if personal data shared by their home countries with the US government were unlawfully disclosed.

Subsequently, legislation has been introduced in both the House of Representatives and the US Senate entitled the Judicial Redress Act of 2015. This bill -- if passed into law -- would extend the benefits of the Privacy Act of 1974 to all citizens of major US allies to seek remedy in US

[69] The Washington Post, "USA Freedom Act: What's in, what's out", 2. June 2015, http://www.washingtonpost.com/graphics/politics/usa-freedom-act/
The authority for bulk collection extends beyond the metadata for an individual telephone subscriber and permits "two hops" of communications records from the target (i.e. all numbers in contact with the target, and all numbers in contact with the numbers in contact with the target.)
[70] See footnote 30.
[71] H.R.1428 - Judicial Redress Act of 2015, https://www.congress.gov/bill/114th-congress/house-bill/1428
[72] US Department of Justice, "Attorney General Holder Pledges Support for Legislation to Provide E.U. Citizens with Judicial Redress in Cases of Wrongful Disclosure of Their Personal Data Transferred to the U.S. for Law Enforcement Purposes", 25. June 2014, http://www.justice.gov/opa/pr/attorney-general-holder-pledges-support-legislation-provide-eu-citizens-judicial-redress

courts of their privacy rights are violated by an agency of the US government. This reciprocal right is already extended to US citizens to access European courts in many cases. The law is intended to establish trust and certainty for allied countries engaged in sharing information with the US government for mutual law enforcement purposes.[73]

Part 3: Conclusion - A Common Search for Legitimacy

The US has experienced a robust debate over privacy and civil liberties standards for intelligence collection in the last two years. And while much of that debate has focused on how US intelligence has been violating the privacy rights of US persons (in pursuit of foreign intelligence targets), there has been significant attention paid to restoring trust and confidence in the legitimacy of US law governing the surveillance of foreign citizens. The reforms proposed and initiated by the Obama administration and the US Congress have narrowed the gap between the standards applied to US citizens and non-US citizens, but it remains wide.

While few Europeans would support the claim that the US policy reforms of intelligence collection practices are sufficient to address their concerns, it is undeniable that Washington has made a wide variety of efforts to change. None of these individual efforts is a decisive shift in approach. The discrimination problem that I identified as a main problem from a German perspective remains a huge challenge. But the cumulative effect of the Obama administration's reviews, investigations, procedural changes, improved standards, transparency, and public documentation of policy and practice all combine to form a baseline for global privacy and security policy. All future reform efforts in the US and elsewhere will be compared to this baseline.

No country can credibly call for reform or claim greater legitimacy that has not met or exceeded the baseline created by the Obama administration. Even though it is an uncomfortable truth in the European response to the Snowden disclosures, many European countries have so far been reluctant to critically examine their own practices. While everyone who cares about privacy has good reasons to remain concerned about NSA surveillance, the reluctance of European countries to engage in a thorough debate about their own practices and the failure to set higher standards for legitimate legal frameworks put European governments in a weak position to challenge US practices.

Thanks to the work of this committee there has been a robust debate about the legal frameworks of the BND as well as its operational practices and its oversight in Germany. The committee has engaged in similar fact finding activities that have informed the reports of the White House Review Group and the Privacy and Civil Liberties Oversight Board. It has heard experts, investigated practices and legal frameworks, and increased transparency. Notably, the Committee has uncovered significant legal shortcomings in the authorization of BND foreign

[73] Chris Murphy, "Murphy, Hatch introduce Judicial Redress Act of 2015", 17. June 2015, http://www.murphy.senate.gov/newsroom/press-releases/murphy-hatch-introduce-judicial-redress-act-of-2015

surveillance -- much as the Review Group and PCLOB did.[74] And the committee has uncovered a wide discrepancy between what the public and its representatives know about surveillance practices, and what is actually being done in the digital age with expanded technological capabilities.

The key question is whether and how Germany will address the problems that have been uncovered by this committee. Meaningful reforms would set Germany apart from other European countries and put it in a position to become the first country that can challenge US surveillance standards and practices based on the adoption of a higher standard. From my perspective the reform agenda should include the following points.[75]

- ➢ Extend G10 law and authorization procedures to all surveillance programs;
- ➢ Strengthen the oversight capabilities of the G10 Commission: including a civil liberties advocate in the process of reviewing authorization requests, full time staff support with legal and technical expertise.
- ➢ Declassification and publication of G10 decisions (particularly those addressing novel issues of law or technology);
- ➢ Publication of the government's interpretation of its legal authority under key statutes, the principles guiding surveillance policy, and the purpose and procedural restrictions on surveillance operations;
- ➢ Strengthen parliamentary oversight with professional staff that has both legal and technical expertise and full authority to examine files and ongoing programs on behalf of the oversight committee;

Policies that set new, universal standards of authorization, restrict operational practices with stronger privacy protections, and increase transparency are all steps in the right direction. Addressing the discrimination problem will be at the center of such a reform effort. In the end, Germans care most about the violations of their own privacy by foreign intelligence services. Thus if Germany significantly narrows the gap between the privacy rights of its own citizens and foreigners, it will be in a stronger position to demand similar treatment from close allies and partners including the United States.

The US government has begun to address the discrimination problem. PPD 28 states that non-US persons will be afforded the same protections as US citizens "to the maximum extent feasible consistent with the national security." This is the baseline. PPD 28 does not guarantee foreigners the same rights and protections as US-persons. But the US government has identified equal treatment as an important principle that should guide the operational practices of foreign intelligence collection. To my knowledge no other government has published a similar

[74] Matthias Bäcker, "Erhebung, Bevorratung und Übermittlung von Telekommunikationsdaten durch die Nachrichtendienste des Bundes", *Stellungnahme zur Anhörung des NSA-Untersuchungsausschusses*, 22. May 2014, https://www.bundestag.de/blob/280844/35ec929cf03c4f60bc70fc8ef404c5cc/mat_a_sv-2-3-pdf-data.pdf

[75] Markus Löning, "Eine Reformagenda für die deutschen Geheimdienste: rechtsstaatlich, demokratisch, effektiv", stiftung neue verantwortung, 15. April 2015, http://www.stiftung-nv.de/publikation/eine-reformagenda-f%C3%BCr-die-deutschen-geheimdienste

document that addresses the question of what kind of policies and standards constrain the collection, analysis, storage and dissemination of foreign national's data.

It is not surprising that governments around the globe have been reluctant to address the discrimination problem. Liberal democracies usually have good legal frameworks governing the authorization, practice, and oversight of surveillance in regard to their own citizens. Extending these legal frameworks to intelligence operations targeting foreigners would greatly improve the privacy protections of these foreigners but also force intelligence agencies to take a much more targeted approach to intelligence collection. This could put severe constraints on how collected data could be analyzed, stored and disseminated. But this does not mean that it cannot be done. And many critics of current intelligence practices argue that it would have beneficial effects, focusing intelligence collection to take a much more strategic and targeted approach rather than amassing ever greater haystacks with the hope of eventually finding the needles.

The work of this committee has put Germany in a strong position to be the first country that goes significantly beyond the policies and standards adopted by the US in the past two years. At its first public hearing, prominent constitutional law experts stated that the German Constitution requires the German government to extend constitutional protections of the privacy of communications (Article 10) beyond Germany and German citizens to any foreigner affected by surveillance conducted by German state authorities.[76] Many parliamentarians and government officials, including the German minister of Justice, have publicly declared that the legal framework and oversight for the BND are in need of a major overhaul.[77]

A few weeks ago the Social Democratic Party (SPD) announced a major step forward towards addressing the discrimination problem. The SPD presented a concept paper that recognizes the constitutional obligations under Article 10 and calls for the extension of the applicability of the G10 law to all foreign surveillance programs -- not just those where one of the communication lines begins or ends in Germany.[78] The institutional reforms needed to achieve this result -- including the expansion of the capacity of the G10 commission to review surveillance authorization requests -- would open the door for setting clear standards of operational restrictions, transparency, and oversight. If this proposal would become the basis for reform, Germany would set a new standard internationally and draw attention to new ideas for modernizing privacy and security policy in democratic societies.

---

[76] See footnote 74; Hans-Jürgen Papier, "Gutachtliche Stellungnahme", *Beweisbeschluss SV-2 des ersten Untersuchungsausschusses des Deutschen Bundestages der 18. Wahlperiode*, 16. May 2014, https://www.bundestag.de/blob/280842/9f755b0c53866c7a95c38428e262ae98/mat_a_sv-2-2-pdf-data.pdf

[77] Jochen Gaugele, "BND einer demokratischen Kontrolle unterwerfen", *Die Welt*, 17. May 2015, http://www.welt.de/politik/deutschland/article141009902/BND-einer-demokratischen-Kontrolle-unterwerfen.html

[78] SPD Bundestagsfraktion, "Eckpunkte der SPD-Bundestagsfraktion für eine grundlegende Reform der Strategischen Fernmeldeaufklärung des BND mit internationaler Vorbildwirkung", 16. June 2015, http://www.spdfraktion.de/sites/default/files/2015-06-16-eckpunkte_reform_strafma-r-endfassung.pdf

Germany and the US are embarked on a similar project in this respect -- to establish laws that are not only adequate for the protection privacy and security for the nation but which are viewed as legitimate in the eyes of the public at home and abroad. This will require establishing democratic principles to constrain the power of digital surveillance under the due process of law. It will require transparency in processes of authorization and operation. And it will require strong oversight and accountability to persuade a skeptical public that the application of power in the digital world is effectively controlled.

The Obama administration has conducted a thorough review of its policies and practices, implemented reforms, and set a new global standard for transparent policies regarding foreign intelligence collection. These are significant steps toward reestablishing legitimacy, and there is a long way left to go. But it is unlikely that America will walk that path alone. It will need a partner like Germany to show both leadership and partnership. Alignment of views and practices between our two countries would be a powerful message to the international community because we approach the questions of privacy and security from profoundly different places.

To understand the NSA's position in American political culture requires an understanding of the idea of American exceptionalism. Put simply, American nationalism celebrates its own military power. Post 9/11 – this feeling has grown even stronger even as the government moved to maximize hard power capabilities. This means the military and the intelligence agencies – even when they behave badly – enjoy relatively uncritical public support. Consider how the military and espionage are represented in pop culture. The NSA does not enjoy the exalted status of Seal Team 6 – but it is a part of the same political zeitgeist. And although many Americans are concerned about the vast system of NSA surveillance; others are proud that we are the best at what we do. And some Americans fit into both categories despite the contradiction.

Now consider "German exceptionalism." German nationalism is a kind of anti-nationalism with respect to military power – for obvious reasons. This is rooted in the experience that democracy is not necessarily a self-correcting form of government. More simply put – the illegitimate use of power can become uncontrolled radicalism. The powers wielded by the NSA would have been a recipe for even further horrors in 20th century German history. Therefore, deeply rooted in Germany's post-war identity is a commitment to restricting the hard power of the state. In my view, this is why Germany -- unlike almost every other country on the planet -- cannot let go of the Snowden story.

Herein lies the conundrum -- stated in dramatic fashion: Americans see the potency of intelligence agencies as a reflection of American exceptionalism; and Germans see the control over these same powers as a reflection of their own exceptionalism. Against the backdrop of these political cultures, we must evaluate the reform debate and assess the prospects for long term change. In this context, it is not surprising that initial reform efforts from Washington would be moderate. And it is not surprising that the reaction of the German public to the NSA debate is sustained outrage. What is surprising is that a parallel reform agenda in Germany has not yet received serious attention. This comparison does not excuse the modesty of American reforms measured against the power of its intelligence operations. However, in the absence of other

national reform efforts, America has set the bar for legal restrictions and transparency. And this does lead to the inevitable conclusion that if America's record of modest reforms sets the global standard (which it does), no nation that fails to better this standard can credibly ask Washington for more.

This analysis of American reform efforts shows that there is room for leadership in democratic societies to challenge all of our assumptions about security and liberty. This Inquiry Committee has done extraordinary work in this regard. If the depth and intensity of these investigations lead to a commensurate reform agenda, Germany will occupy a position of global leadership in modernizing policies of privacy and security in the digital world. That achievement will be a credit to the principles of the German public and a great contribution to the long term stability and moral authority of the transatlantic alliance.

Appendix: Official US government documents regarding surveillance reform

Acts, Directives and Orders

PATRIOT Act

- H.R. 3162, “Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001” http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=107_cong_bills&docid=f:h3162enr.txt.pdf
- US Court of Appeals for The Second Circuit, Ruling regarding Section 215 (USA PATRIOT Act) http://www.ca2.uscourts.gov/decisions/isysquery/5b758b27-c77d-44a2-b6e5-dbf456f5c142/1/doc/14-42_complete_opn.pdf

Foreign Intelligence Surveillance Act (FISA)

- Public Law 95-511, “Foreign Intelligence Surveillance Act of 1978”, http://www.gpo.gov/fdsys/pkg/STATUTE-92/pdf/STATUTE-92-Pg1783.pdf

USA Freedom Act

- H.R.2048 - USA FREEDOM Act of 2015, Public Law No: 114-23 (06/02/2015) https://www.congress.gov/bill/114th-congress/house-bill/2048/text

Judicial Redress Act

- H.R.1428 - Judicial Redress Act of 2015, Introduced in House 18. March 2015 https://www.congress.gov/bill/114th-congress/house-bill/1428

Presidential Policy Directive - Signals Intelligence Activities (PPD-28)

- White House Press Release and Policy Directive https://www.whitehouse.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities
- Office of the Director of National Intelligence, “2015 Anniversary Report”, 3. February 2015 http://icontherecord.tumblr.com/ppd-28/2015/overview

Executive Order 12333

- United States Intelligence Activities, Federal Register Vol. 40, No. 235 (December 8, 1981), amended by EO 13284 (2003), EO 13355 (2004), and EO 13470 (2008) http://www.dni.gov/index.php/about/organization/ic-legal-reference-book-2012/ref-book-eo-12333

Reports

The President's Review Group on Intelligence and Communications Technologies

- Report: Liberty and Security in a Changing World, 12. December 2013
  https://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf

Privacy and Civil Liberties Oversight Board

- Document Library: https://www.pclob.gov/library.html
- Report on the Telephone Records Program Conducted under Section 215 of the USA PATRIOT Act and on the Operations of the Foreign Intelligence Surveillance Court
  https://www.pclob.gov/library/215-Report_on_the_Telephone_Records_Program.pdf
- Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act
  https://www.pclob.gov/library/702-Report.pdf
- Recommendation Assessment Report
  https://www.pclob.gov/library/Recommendations_Assessment-Report.pdf
  https://www.pclob.gov/library/Recommendations_Assessment-FactSheet.pdf

National Academy of Sciences / National Research Council

- National Research Council, "Bulk Collection of Signals Intelligence: Technical Options", 15. January 2015,
  http://www.nap.edu/openbook.php?record_id=19414

Declassified Documents

- Release of Documents Concerning Activities under the Foreign Intelligence Surveillance Act, http://icontherecord.tumblr.com/post/112610953998/release-of-documents-concerning-activities-under
- US Foreign Intelligence Surveillance Court, Docket Number 702(i)-08-01, Memorandum Opinion, 4. September 2008,
  http://www.dni.gov/files/documents/0315/FISC%20Opinion%20September%204%202008.pdf
- U.S. Foreign Intelligence Surveillance Court, "Minimization Procedures used by NSA in Connection with FISA Section 702", 31. October 2011
  https://www.aclu.org/sites/default/files/field_document/minimization_procedures_used_by_nsa_in_connection_with_fisa_sect_702.pdf
- National Security Agency, "Overview of Signals Intelligence Authorities", 19. September 2014,
  https://www.aclu.org/files/assets/eo12333/NSA/Overview%20of%20Signals%20Intelligence%20Authorities.pdf
- List of declassified FISC opinions can also be found at
  https://epic.org/privacy/surveillance/fisa/fisc/#orders