CONGRESSIONAL TASKFORCE ON TERRORISM AND UNCONVENTIONAL WARFARE

Parliamentary Intelligence-Security Forum
September 17 - 19
Washington, DC

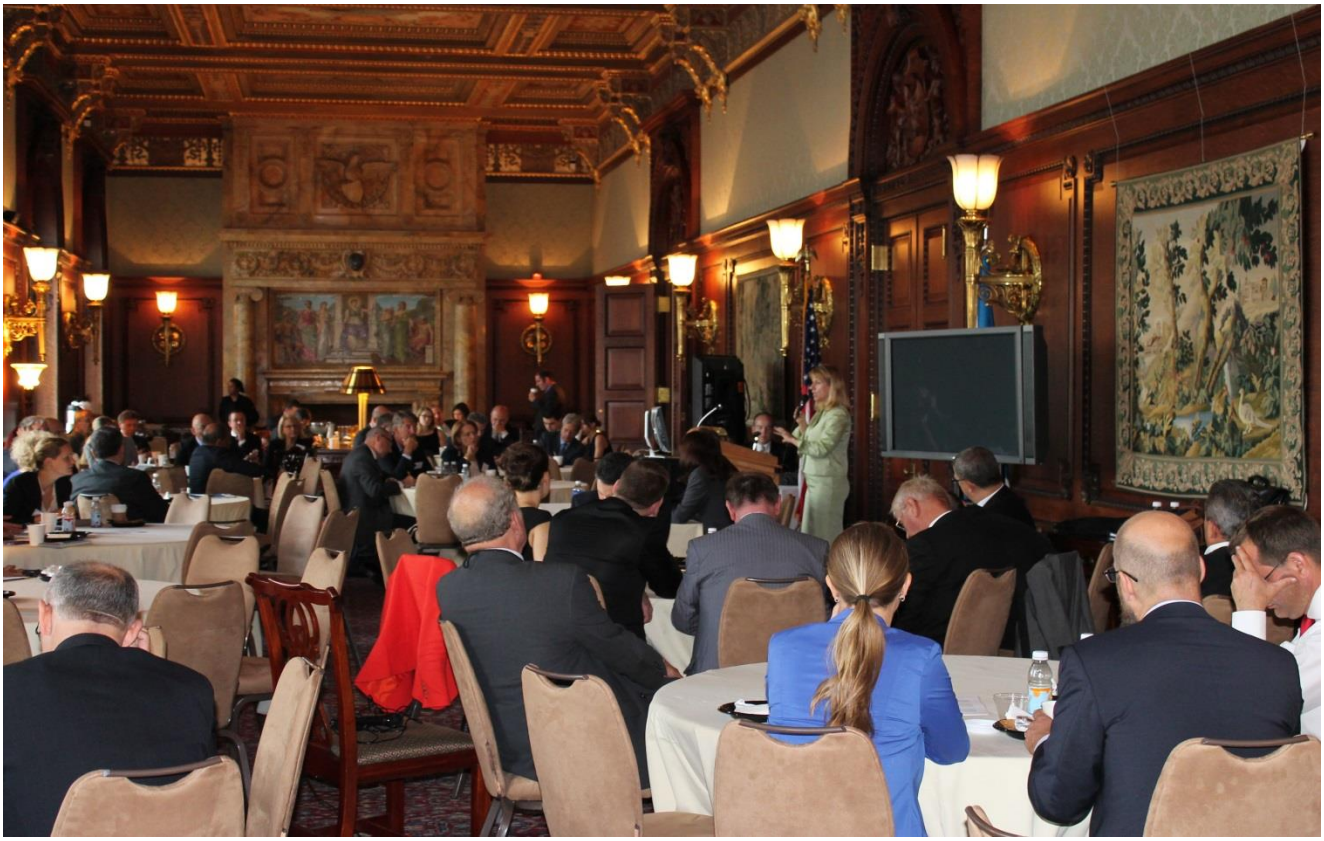
2014 Annual Report

THE HONORABLE ROBERT M. PITTENGER
Chairman

FOR MORE INFORMATION:
(202)225-1976

PARLIAMENTARY INTELLIGENCE SECURITY FORUM

2014 Annual Report



The Need for Dialogue

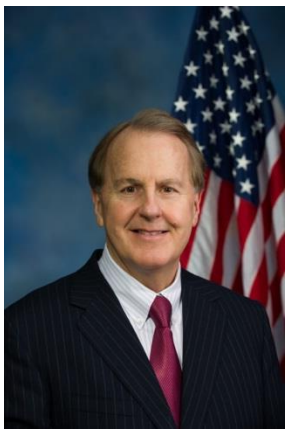
As Chairman of the Congressional Taskforce on Terrorism and Unconventional Warfare, I spent many hours discussing the issues of national security and intelligence policy – with colleagues in Congress, security experts, and with foreign diplomats. These conversations all revealed a similar undertone, the need for further dialogue.

While in Vienna in December, 2013, I met with Members of the Austrian Parliament who made clear their desire to engage in these discussions with their American counterparts. In June 2014, a delegation of five Austrian Parliamentarians visited Washington, D.C. to do just that. An afternoon of meaningful dialogue ignited the need for a greater, more inclusive forum with European allies in the fight against global terrorism.

To this end, we hosted the first Parliamentary Intelligence-Security Forum at the Library of Congress in Washington, D.C. where diplomats from 28 countries spent three days discussing the needs, concerns and realities regarding U.S. – European intelligence efforts.

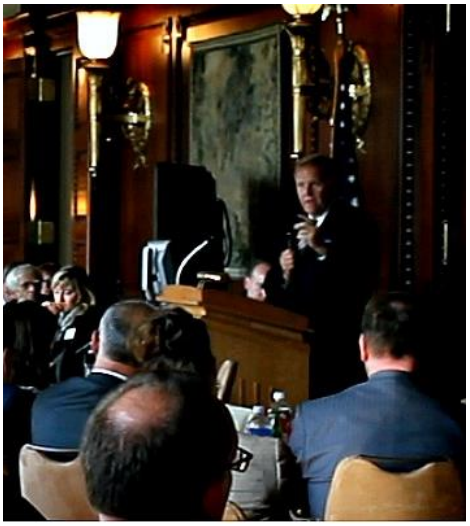
With deep gratitude and respect, we honor the important work of Chairman Mike Rogers with his leadership of the House Permanent Select Committee on Intelligence. Chairman Rogers provided me the opportunity to initiate and lead this Forum with our European allies. His thoughtful analysis of intelligence and security issues has been a critical component to the protection of our homeland and vital American and allied interests around the world.

Robert Pittenger
Member of Congress
Chairman, Congressional Taskforce on Terrorism
and Unconventional Warfare



Executive Summary

The Parliamentary Intelligence-Security Forum provided an opportunity for legislators, Ambassadors, Executive officials, and intelligence experts to engage in meaningful and open dialogue on the issues of intelligence policy and threats to international security.



America's European allies heard presentations from Members of Congress from both sides of the aisle, and the White House. The White House was represented by the Office of the Director of National Intelligence. Dignitaries also heard from the Privacy and Civil Liberties Oversight Board, a bipartisan independent agency focused on ensuring we maintain the correct balance between security and privacy, as well as former White House officials from both the President Bush and President Obama Administrations, and other experts of intelligence and security policy. Each official commented on the intelligence policies of the United States and our commitment to civil liberties as we seek to maintain security.

Participants included:

Congressional Leadership:
House Intelligence Chairman Rogers
House Intelligence Ranking Member Ruppersberger
House Judiciary Chairman Goodlatte

Members of Congress:
Congressman Devin Nunes
Republican, House Intelligence Committee
Congressman Jim Himes
Democrat, House Intelligence Committee

Executive Officials:
Mr. Robert Litt, General Counsel, *Office of the Director of National Intelligence*
Mr. Alexander Joel, Civil Liberties Protection Officer, *Office of the Director of National Intelligence*
David Medine, Chairman, *Privacy and Civil Liberties Oversight Board*
Rachel Brand, Board Member, *Privacy and Civil Liberties Oversight Board*

Important to this forum was the focus on creating dialogue with an exchange of questions and answers, rather than utilizing a lecture style briefing. Members of Parliament and Ambassadors from each country actively participated in each session of the forum – presenting the concerns of their respective countries and confronting U.S. officials with the hard questions for which they had been seeking answers. European officials engaged in constructive dialogue on the threats facing each of our nations today and how privacy concerns must be factored in to intelligence policy.

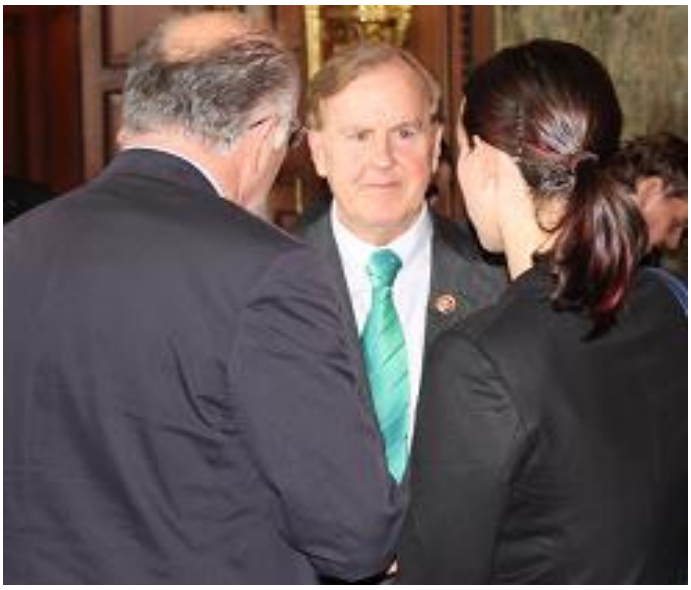
Given the attention U.S. intelligence policy has received in recent years, concern was raised by many U.S. allies regarding the protection of civil liberties of non-U.S. citizens. These concerns were addressed, and the commitment to further dialogue regarding these concerns was made by all participants at future Parliamentary Intelligence-Security Forums, as noted by enclosed letters from attending delegates. Also included in the Parliamentary Intelligence-Security Forum 2014 Annual Report are alternate executive agency reports conveying the protections America is providing in recent years to the civil liberty concerns of non-U.S. citizens.

See Addendum: Privacy and Civil Liberties Oversight Board; July 21, 2014

Summary of Discussion

The overall discussion of the Parliamentary Intelligence-Security Forum can be divided into two distinct topics:

- The current threats facing each of the allied nations participating in the Parliamentary Intelligence-Security Forum
- Intelligence policy as it relates to civil liberties



Over three days, Members of Parliament, Ambassadors, Member of Congress, Executive officials, and policy experts discussed the common views shared by all, as well as sought to work through points of disagreement.

The Threats We Face

There was great consensus by all that each of our nations is facing imminent threats from rogue nations and terrorist organizations. On the opening day of the Parliamentary Intelligence-Security Forum, President Petro Poroshenko of Ukraine addressed a joint–session of Congress, reminding the world that Russian aggression will not stop with the annexation of Crimea. Many dignitaries during the forum shared their nations' similar concerns that Russia is seeking to reclaim the borders once maintained by the Soviet Union. Nuclear proliferation, especially with regards to Iran, was another topic participants agreed would create further instability in the Middle East and pose great threats to peaceful nations.

The Parliamentary Intelligence-Security Forum also took place in the beginning days as a coalition was formed to take action against ISIS. The threat of ISIS was acknowledged given its expansive financial resources, primarily from extortion. ISIS is armed with sophisticated technology, which poses new and greater threats for democratic nations. The introduction of social media into the arsenal of terrorists is a new development, which has spurred the influx of foreign fighters to the region. With thousands of Western citizens crossing into Syria and becoming radicalized, we face the threat of terrorists with the ability to freely travel to and from our nations with Western passports. This unique threat supports the critical objective to gather intelligence and the need for continued cooperation as we seek to protect our nations.

Civil Liberties Concerns

Members of Parliament reported their concern that the United States is not taking appropriate steps to maintain civil liberties when engaging in intelligence operations. Many of these concerns stem from media reports which have not accurately portrayed the U.S. efforts – however the concerns they created are real and America must work to ensure they receive an appropriate response. During

the Forum participants were provided a detailed overview of how the United States directs and oversees its intelligence activities. U.S. officials reiterated the importance of maintaining civil liberties, and acknowledge security can be achieved without infringing on those liberties. Foreign dignitaries heard from multiple experts, Members of Congress, and Executive officials regarding the existing framework of law and policies in place to regulate the Intelligence Community. This explanation included an in depth discussion of the multiple layers of oversight by each of the three branches within the United States government – Executive, Legislative, and Judicial. Chairman Goodlatte gave specific insight to his role as Chairman of the Judiciary Committee and the oversight and effectiveness of the Foreign Intelligence Surveillance Court.

American officials also spoke directly to the framework already in place to protect privacy, not just for Americans, but for all individuals. House Intelligence Chairman Rogers and Ranking Member Ruppersberger both reiterated, with emphasis, the United States has not and does not engage in mass spying on all citizens of European nations, nor does the United States maintain the capacity or desire to do so. The laws governing the Intelligence Community already in place provide extensive protections for the privacy and civil liberties of non-U.S. individuals. Contained in this 2014 annual report are two reports from the Office of the Director of National Intelligence and the Privacy and Civil Liberties Oversight Board to provide further in-depth analysis of the existing provisions.

See addendum: Office of the Director of National Intelligence; July 2014

Additional Discussion Topics:

Oversight of Intelligence Community:

The Forum contained an overview of the 17 agencies within the United States Intelligence Community, as well as the structure of oversight by the Executive, Legislative, and Judicial branches of the Federal government. Members of Congress, Executive officials, and experts provided background on how the United States maintains one of the most restrictive and transparent intelligence gathering systems in the world. Members from the House Intelligence Permanent Select Committee also gave insight into the inner workings of the Committee's role in direct oversight of the Intelligence Community. Particular attention was given to the differences by which Congress oversees intelligence activities when compared to the oversight provided by Parliaments throughout Europe of their respective intelligence agencies. Delegates also learned the functions of the Federal Intelligence Surveillance Court as part of the judicial oversight, and heard from two executive agencies as to the role of the Executive branch in oversight of the Intelligence Community.

The level of oversight exhibited over U.S. intelligence agencies by the United States Congress is unparalleled by other legislative bodies. Instances of cooperation were noted by U.S. speakers, pointing to the efforts foreign intelligence agencies in Europe are engaged in, in cooperation with the United States. These efforts of European agencies are however, not under the same level of oversight by European Parliaments as is provided by the United States Congress for U.S. agencies. As was noted by foreign delegates, further oversight of their respective agencies is needed to ensure debates regarding U.S. efforts are fair and balanced.

Legislative Issues

The Forum highlighted specific existing legislation, which currently provides for substantial civil liberties protections. Members of Congress emphasized new legislation aimed to create additional oversight and transparency. Officials from the Executive branch further pointed to Presidential Policy Directive 28, making clear the United States' commitment to the protection of personal information for all people, not just U.S. citizens.

The Patriot Act and the Foreign Intelligence Surveillance Act publicly detail requirements and limitations posed on the intelligence agencies of the United States. In 2008, years prior to any reports of Snowden-leaked information, the United States had already enacted legislation to tighten procedures which apply to foreign targets. The FISA Amendments Act requires approval by a U.S. court to gather intelligence domestically on foreign persons outside of the United States. The discussions on these laws has created greater scrutiny of American intelligence gathering practices through robust debate, than what has been provided in other countries. In May of 2014, the House of Representatives passed the USA Freedom Act, creating further protections of civil liberties and adding further oversight and transparency to intelligence agencies. Further, the USA Freedom Act would prevent the bulk collection of data by the United States government and only allow data to be retained by independent companies.

Information Sharing

Participants of the Forum spent time discussing the need for information sharing among allies. The dialogue focused on the already existing relationships of information sharing, both from the United States to our allies, and from our allies to the United States. Emphasis was given to how information sharing plays out in efforts to prevent proliferation of nuclear weapons, terrorist financing and terrorist attacks. U.S. officials also focused specifically on the nearly fifty instances U.S. intelligence efforts disrupted terrorist attacks around the world, through sharing information with our allies. By percentage, the largest numbers of disruptions have in fact been through the sharing of information with Germany. The continued partnership of allies through information sharing is vital as we cooperate to end the common threats shared by all peaceful nations.

Snowden Leaks

Discussions at the Forum related to Edward Snowden, and the harm caused by the information he leaked. Those discussions centered on the damage to national security for both the United States and European allies. Edward Snowden stole up to 1.8 million documents, including military operations from the United States Army, Navy, Air Force and Marines. Given Snowden travelled through China, and is now being hosted by the Russian government, we all must assume this information has been disclosed to our adversaries. Had Snowden's real intent been the protection of civil liberties, a number of possible alternatives existed for him to take actions that would not have placed Europe and America at risk.

Supplemental Addendum Excerpts

Privacy and Civil Liberties Oversight Board
"Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act"
July 2, 2014
Report in its entirety: http://www.pclob.gov/Library/702-Report.pdf

Excerpt

IV. Analysis of Treatment of Non-U.S. Persons

The treatment of non-U.S. persons under U.S. surveillance programs raises important but difficult legal and policy questions. Privacy is a human right that has been recognized most prominently in the International Covenant on Civil and Political Rights ("ICCPR"), an international treaty ratified by the U.S. Senate. Many of the generally applicable protections that already exist under U.S. surveillance laws apply to U.S. and non-U.S. persons alike. The President's recent initiative under Presidential Policy Directive 28 on Signals Intelligence ("PPD-28")[439] will further address the extent to which non-U.S. persons should be afforded the same protections as U.S. persons under U.S. surveillance laws. Because PPD-28 invites the PCLOB to be involved in its implementation, the Board has concluded that it can make its most productive contribution in assessing these issues in the context of the PPD-28 review process.

A. Existing Legal Protections for Non-U.S. Persons' Privacy

A number of provisions of Section 702, as well as provisions in other U.S. surveillance laws, protect the privacy of U.S. and non-U.S. persons alike. These protections can be found, for example, in (1) limitations on the scope of authorized surveillance under Section 702; (2) damages and other civil remedies that are available to subjects of unauthorized surveillance as well as sanctions that can be imposed on government employees who engage in such conduct; and (3) prohibitions on unauthorized secondary use and disclosure of information acquired pursuant to the Section 702 program. These sources of statutory privacy protections are discussed briefly.

The first important privacy protection provided to non-U.S. persons is the statutory limitation on the scope of Section 702 surveillance, which requires that targeting be conducted only for purposes of collecting foreign intelligence information.[440] The definition of foreign intelligence information purposes is limited to protecting against actual or potential attacks; protecting against international terrorism, and proliferation of weapons of mass destruction; conducting counter-intelligence; and collecting information with respect to a foreign power or foreign territory that concerns U.S. national defense or foreign affairs.[441] Further limitations are imposed by the required certifications identifying the specific categories of foreign intelligence information, which are reviewed and

---

439 Presidential Policy Directive — Signals Intelligence Activities, Policy Directive 28, 2014 WL 187435 (Jan. 17, 2014) ("PPD-28"), *available at* http://www.whitehouse.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities.

440 50 U.S.C. § 1881a(a).

441 50 U.S.C. § 1801(e).

approved by the FISC.[442] These limitations do *not* permit unrestricted collection of information about foreigners.

The second group of statutory privacy protections for non-U.S. persons are the penalties that apply to government employees who engage in improper information collection practices — penalties that apply whether the victim is a U.S. person or a non-U.S. person. Thus, if an intelligence analyst were to use the Section 702 program improperly to acquire information about a non-U.S. person (for example, someone with whom he or she may have had a personal relationship), he or she could be subject not only to the loss of his or her employment, but to criminal prosecution.[443] Finally, a non-U.S. person who was a victim of a criminal violation of either FISA or the Wiretap Act could be entitled to civil damages and other remedies.[444] In sum, if a U.S. intelligence analyst were to use the Section 702 program to collect information about a non-U.S. person where it did not both meet the definition of foreign intelligence and relate to one of the certifications approved by the FISA court, he or she could face not only the loss of a job, but the prospect of a term of imprisonment and civil damage suits.

The third privacy protection covering non-U.S. persons is the statutory restriction on improper secondary use found at 50 U.S.C. § 1806, under which information acquired from FISA-related electronic surveillance may not "be used or disclosed by Federal officers or employees except for lawful purposes."[445] Congress included this language "to insure that information concerning foreign visitors and other non-U.S. persons . . . is not used for illegal purposes."[446] Thus, use of Section 702 collection for the purpose of suppressing or burdening criticism or dissent, or for disadvantaging persons based on their ethnicity, race, gender, sexual orientation, or religion, would violate Section 1806.

Further, FISA provides special protections in connection with legal proceedings, under which an aggrieved person — a term that includes non-U.S. persons — is required to be notified prior to the disclosure or use of any Section 702–related information in any

---

442 50 U.S.C. § 1881a(g)(2)(A)(v).

443 *See* Bates October 2011 Opinion, *supra*, at 17 n.15, 2011 WL 10945618, at *6 n.15 (criminal penalties of 50 U.S.C. § 1809 of the FISA are implicated by Section 702 surveillance that strays beyond the scope of the court's order approving such activities). In addition, to the extent that Section 702 program surveillance strayed from the certifications approved by the FISA court, it would potentially implicate the criminal provisions of the Wiretap Act, 18 U.S.C. § 2511(1), because the Section 702 surveillance would then lose its safe harbor for authorized FISA activities under Section 2511(2)(e) of the Wiretap Act.

444 *See* 50 U.S.C. § 1810 ("aggrieved person" not limited to U.S. persons); 18 U.S.C. § 2520 ("any person" not limited to U.S. persons); *see also Suzlon Energy Ltd. v. Microsoft Corp.*, 671 F.3d 726, 728-29 (9th Cir. 2011) (construing the statutory term "any person" to include non-U.S. persons).

445 50 U.S.C. § 1806(a) (incorporated into Section 702 by 50 U.S.C. § 1881e(a)).

446 H.R. Rep. No. 95-1283(I), at 88-90 (1978) (discussing Section 106 of H.R. 7308, which became Section 106 of the FISA).

federal or state court.[447] The aggrieved person may then move to suppress the evidence on the grounds that it was unlawfully acquired and/or was not in conformity with the authorizing Section 702 certification.[448] Determinations regarding whether the Section 702 acquisition was lawful and authorized are made by a United States District Court, which has the authority to suppress any evidence that was unlawfully obtained or derived.[449]

Finally, as a practical matter, non-U.S. persons also benefit from the access and retention restrictions required by the different agencies' minimization and/or targeting procedures. While these procedures are legally required only for U.S. persons, the cost and difficulty of identifying and removing U.S. person information from a large body of data means that typically the entire dataset is handled in compliance with the higher U.S. person standards.

B. President's Initiative to Protect the Privacy of Non-U.S. Persons

As a matter of international law, privacy is a human right that has been recognized most prominently in the ICCPR, an international treaty ratified by the U.S. Senate. The question of how to apply the ICCPR right of privacy to national security surveillance, however, especially surveillance conducted in one country that may affect residents of another country, has to this point not been settled among the signatories to the treaty and is the subject of ongoing spirited debate.[450]

The executive branch is currently engaged in an extensive review of the extent to which, as a policy matter, the United States should afford all persons, regardless of nationality, a common baseline level of privacy protections in connection with foreign intelligence surveillance. This review began on January 17 of this year, when President Obama issued PPD-28,[451] in which he directed the review of the treatment of information regarding non-U.S. persons in connection with its surveillance programs.

Issues relating to the treatment of non-U.S. persons in government surveillance programs are by no means limited to the Section 702 program. Questions arise in

---

447 *See* 50 U.S.C. § 1806(c), (d).

448 50 U.S.C. § 1806(e).

449 50 U.S.C. § 1806(f), (g).

450 The United States currently interprets the ICCPR as not applying extra-territorially. Nonetheless the Board has received thoughtful comments and testimony arguing to the contrary. The Board also notes that in November 2013, the United Nations adopted, with United States support, a Resolution on "The right to privacy in the digital age." This resolution includes a provision requesting that the United Nations High Commissioner for Human Rights develop and present a report examining "the protection and promotion of the right to privacy in the context of domestic and extraterritorial surveillance and/or interception of digital communications and collection of personal data, including on a mass scale." This report is expected to be presented in August 2014.

451 PPD-28, *supra*.

connection with signals intelligence conducted under other statutes and programs, including Executive Order 12333. Under PPD-28, the government has begun to address, as a matter of policy, the privacy and civil liberties of non-U.S. persons in connection with the full spectrum of signals intelligence programs conducted by the United States. The introduction to that directive notes that "signals intelligence activities must take into account that all persons should be treated with dignity and respect, regardless of their nationality or wherever they might reside, and that all persons have legitimate privacy interests in the handling of their personal information."[452] The government is presently in the process of implementing the principles set forth in that directive, including the requirement that "signals intelligence activities shall be as tailored as feasible."[453] PPD-28 sets forth a number of principles that have historically been, or will be, implemented, among them:

> Privacy and civil liberties shall be integral considerations in the planning of U.S. signals intelligence activities. The United States shall not collect signals intelligence for the purpose of suppressing or burdening criticism or dissent, or for disadvantaging persons based on their ethnicity, race, gender, sexual orientation, or religion. Signals intelligence shall be collected exclusively where there is a foreign intelligence or counterintelligence purpose to support national and departmental missions and not for any other purposes.[454]

Further, PPD-28 provides that:

> 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.[455]

The Intelligence Community has already begun reviewing various options for implementing PPD-28, and the Board will engage in this process. PPD-28 specifically provides for direct PCLOB participation:

> The Privacy and Civil Liberties Oversight Board is encouraged to provide [the President] with a report that assesses the implementation of any matters contained within this directive that fall within its mandate.[456]

---

452 PPD-28, *supra*.

453 PPD-28, *supra*, § 3(d).

454 PPD-28, *supra*, § 3(b).

455 PPD-28, *supra*, § 4.

456 PPD-28, *supra*, § 5(b).

The Board has thus concluded that the optimal way for it to assess the treatment of information of non-U.S. persons is in the broader context of the PPD-28 review where it can evaluate other surveillance programs, along with Section 702, with a view to an integrated approach to foreign subjects of surveillance and the collection of signals intelligence. The implementation of PPD-28 may change the way Section 702 is operated and in so doing alleviate some of the concerns that have been voiced about its treatment of non-U.S. persons.

Supplemental Addendum Excerpts

Office of the Director of National Intelligence
July 2014
"Safeguarding the Personal Information of all People"
Report in its entirety: http://www.dni.gov/files/documents/1017/PPD-28_Status_Report_Oct_2014.pdf

Excerpt

The United States is committed to protecting the personal information of all people around the world, regardless of their nationality. Indeed, it is our longstanding practice to conduct signals intelligence (SIGNIT) activities only for authorized foreign intelligence and counter intelligence purposes, and to safeguard information obtained through such means from unauthorized access or disclosure. On January 17, 2014, the President issued Presidential Policy Directive (PPD)-28, Signals Intelligence Activities, which "articulates principles to guide why, whether, when and how the United States conducts SIGINT activities for authorized foreign intelligence and counterintelligence purposes." This directive reinforces current practices, establishes new principles that govern how the United States conducts SIGINT collection, and strengthens Executive Branch oversight of SIGINT activities. Moreover, the principles ensure that in conducting SIGINT activities, the United States takes into account not only the nation's security requirements, but also the security and privacy concerns of U.S. allies and partners, the increased globalization of trade and investment, and the commitment to protect privacy rights and civil liberties

Interim Progress Report on Implementing PPD-28

Friday, October 17, 2014
By Robert Litt and Alexander W. Joel

As the President said in his speech on January 17, 2014, "the challenges posed by threats like terrorism, proliferation, and cyber-attacks are not going away any time soon, and for our intelligence community to be effective over the long haul, we must maintain the trust of the American people, and people around the world."

As a part of that effort, the President made clear that the United States is committed to protecting the personal information of all people regardless of nationality. This commitment is reflected in the directions the President gave to the Intelligence Community on that same day, when he issued Presidential Policy Directive/PPD-28, *Signals Intelligence Activities.*

New Standards for Safeguarding Privacy

PPD-28 reinforces current practices, establishes new principles, and strengthens oversight, to ensure that in conducting signals intelligence activities, the United States takes into account not only the security needs of our nation and our allies, but also the privacy of people around the world.

The Intelligence Community already conducts signals intelligence activities in a carefully controlled manner, pursuant to the law and subject to layers of oversight, focusing on important foreign intelligence and national security priorities. But as the President recognized, "[o]ur efforts will only be effective if ordinary citizens in other countries have confidence that the United States respects their privacy too."

To that end, the Intelligence Community has been working hard to implement PPD-28 within the framework of existing processes, resources, and capabilities, while ensuring that mission needs continue to be met.

In particular, PPD-28 directs intelligence agencies to review and update their policies and processes - and establish new ones as appropriate - to safeguard personal information collected through signals intelligence, regardless of nationality and consistent with our technical capabilities and operational needs.

Key Privacy Principles for the Intelligence Community

- Ensuring that privacy and civil liberties are integral considerations in signals intelligence activities.
- Limiting the use of signals intelligence collected in bulk to the specific approved purposes set forth in PPD-28.
- Ensuring that analytic practices and standards appropriately require that queries of collected signals intelligence information are duly authorized and focused.
- Ensuring that retention and dissemination standards for United States person information under Executive Order 12333 are also applied, where feasible, to all personal information in signals intelligence, regardless of nationality.
- Clarifying that the Intelligence Community will not retain or disseminate information as "foreign intelligence" solely because the information relates to a foreign person.
- Developing procedures to ensure that unevaluated signals intelligence is not retained for more than five years, unless the DNI determines after careful evaluation of appropriate civil liberties and privacy concerns, that continued retention is in the national security interests of the United States.
- Reinforcing and strengthening internal handling of privacy and civil liberties complaints.
- Reviewing training to ensure that the workforce understands the responsibility to protect personal information, regardless of nationality. Successful completion of this training must be a prerequisite for accessing personal information in unevaluated signals intelligence.
- Developing oversight and compliance programs to ensure adherence to PPD-28 and agency procedures, which could include auditing and periodic reviews by appropriate oversight and compliance officials of the practices for protecting personal information contained in signals intelligence and the agencies' compliance with those procedures.
- Publicly releasing, to the extent consistent with classification requirements, the procedures developed pursuant to PPD-28.

http://www.dni.gov/index.php/newsroom/reports-and-publications/204-reports-publications-2014/1126-interim-progress-report-on-implementing-ppd-28

Presentations

Welcome

Dr. Karen Donfried,
President of the German Marshall Fund

Intelligence Introduction Briefing

House Permanent Select Committee on Intelligence
Mr. Michael Bahar, General Counsel
Mr. Tom Corcoran, Senior Policy Advisor
Mr. Michael Ellis, Republican Counsel

Full Assessment of the ISIS Threat Against the West

Mr. Faysal Itani,
Resident Fellow with Atlantic Council

Mr. Barry Pavel,
Vice President and Director of the Brent Scowcroft Center on International Security at the Atlantic Council
Former special assistant to the president and senior director for defense policy and strategy on the National Security Council (NSC) staff, serving both President George W. Bush and President Barack Obama

Mr. Michael Leiter,
Senior Counselor to the Chief Executive Officer of Palantir Technologies
Former Director of the National Counterterrorism Center (NCTC)

"Conferences like this provide a great opportunity for transatlantic allies and partners to come together and discuss serious security issues such as the rise of the Islamic State. Together, through dialogue and action, we can face these challenges and protect our citizens from the threats of a dynamic and unstable world." – *Mr. Barry Pavel*

Presentations

Intelligence Member Briefing

House Permanent Select Committee on Intelligence

Chairman Mike Rogers, Republican
Ranking Member Dutch Ruppersberger, Democrat
Congressman Devin Nunes, Republican
Congressman Jim Himes, Democrat

"The U.S. and Europe have a longstanding friendship and alliance, and we share vital national security interests in areas like counter-terrorism and counter-proliferation. We must continue to cooperate on security and intelligence matters going forward, and this inter-parliamentary dialogue is important to building and maintaining the trust that is the foundation of that cooperation." – *Chairman Rogers*

"I appreciate the opportunity to speak with a number of leaders from the EU. As we face a number of issues across the globe such as cybersecurity, ISIL, and Ebola, it is critical that we maintain our strong relationship and consider how to work together for positive change moving forward." – *Ranking Member Ruppersberger*

"Europe and the United States face many threats from around the world. Our nations' security, intelligence and elected officials must work together to best address these threats and keep our citizens safe. The Parliamentary Intelligence-Security Forum helped build these crucial relationships between our leaders and I look forward to continuing the discussions between our respective security and intelligence institutions." – *Congressman Jim Himes*

"Europe and the United States should collaborate closely to address the growing security threat posed by international cyber-attacks, particularly from Russia and China." – *Congressman Devin Nunes*

Presentations

The Need for Cooperation

Ms. Samantha Ravich
Former Co-Chair of the National Commission for the Review of Research and Development in the US Intelligence Community

Mr. Michael Allen
Managing Director of Beacon Global Strategies LLC
Former Majority Staff Director of House Permanent Select Committee on Intelligence, Special Assistant to the President and Senior Director for Counter-proliferation Strategy

"When our adversaries are using the same communications as us that route through our countries, there is inevitably great crossover of what information we need to protect ourselves. We need further dialogue, like the Parliamentary Intelligence-Security Forum, to ensure we are addressing the critical needs to protect our nations, while continuing to give proper attention to privacy concerns." – Mr. Michael Allen

"Conferences like this are imperative to talk through differences we have in understanding and prioritizing some of the tradeoffs on privacy and security so we can get to the heart of the matter-- defending against the serious threats against our societies, economies, and citizens." – *Ms. Samantha Ravich*

Briefing – Foreign Intelligence Surveillance Court

House Judiciary Committee
Chairman Bob Goodlatte

"The Parliamentary Intelligence-Security Forum successfully brought together leaders from the U.S. and across Europe to ensure a constructive dialog continues between our countries on the need for intelligence gathering programs that allow law enforcement to intercept true threats while protecting civil liberties." – Chairman Bob Goodlatte

Presentations

Privacy Protections in Place

Privacy and Civil Liberties Oversight Board

Mr. David Medine
Chairman, Privacy and Civil Liberties Oversight Board

Ms. Rachel Brand
Board Member, Privacy and Civil Liberties Oversight Board

"We appreciated the opportunity provided by the Parliamentary Intelligence-Security Forum to share views with European representatives about how to balance national security with privacy and civil liberties and to describe the model the United States has chosen of creating an independent, bipartisan agency to conduct intelligence community oversight. We look forward to continuing this dialogue with the international community." – *Chairman Medine and Board Member Brand*

Please see attached report from the Privacy and Civil Liberties Oversight Board: Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act

Espionage and Transatlantic Politics

Mr. James A. Lewis
Senior fellow and Director of the Strategic Technologies Program at CSIS
Former rapporteur for both the 2010 and 2013 UN Group of Government Experts on Information Security

Ms. Mary DeRosa
Distinguished Visitor from Practice, Georgetown Law
Former Deputy Assistant and Deputy Counsel to the President, and National Security Council Legal Adviser in the Obama Administration

Ms. Heather Conley
Senior Vice President for Europe, Eurasia, and the Arctic; and Director, Europe Program
Deputy assistant secretary of state in the Bureau for European and Eurasian Affairs

Presentations

Legal and Policy Oversight of Intelligence Activities

Office of the Director of National Intelligence
Mr. Robert S. Litt,
General Counsel, *Office of the Director of National Intelligence*

Mr. Alexander W. Joel,
Civil Liberties Protection Officer, *Office of the Director of National Intelligence*

Please see attached report from the Office of the Director of National Intelligence: Safeguarding the Personal Information of all People

Defunding the Threat of Terrorism

Mr. Christopher Griffin
Executive Director for Foreign Policy Imitative

Dr. Emanuele Ottolenghi
Senior Fellow for Foundation for Defense of Democracies

Dr. David Asher
Adjunct Senior Fellow with Center for New American Security
Former advisor Office of the Secretary of Defense, US Special Operations Command, Central Command

"The insights offered by all participants in this Forum is a reminder of the importance of the transatlantic partnership in meeting the challenges of Russia's aggression against its neighbors, the crisis engulfing the Middle East, and the increasing belligerence of China in the Asia-Pacific. Continued discussions like this one will be essential for framing this partnership, and I commend Congressman Pittenger for hosting this important first step." – Christopher Griffin

Enclosed

Letters from Members of Parliament

Finland	Speaker Eero Heinäluoma
Montenegro	President of Parliament, Mr. Ranko Krivokapic
Hungary	Speaker László Kövér
Romania	Speaker, Valeriu Ștefan Zgonea
Spain	President of Congress of Deputies, Jesus Posada Moreno
Sweden	Deputy Speaker Ulf Holm
Austria	Mr. Andreas Karlsboeck
Austria	Mr. Andreas Schieder
Austria	Mr. Peter Pilz
Austria	Mr. Reinhold Lopatka
Finland	Ms. Tuija Brax
Germany	Dr. Patrick Sensburg
Germany	Mr. Wolfgang Bosbach
Germany	Mr. Mahmut Özdemir
Germany	Mr. Hans-Christian Ströbele
Greece	Mr. Kostas Tsiaras
Italy	Mr. Paolo Gentiloni
Lithuania	Mr. Emanuelis Zingeris
Romania	Dr. Gabriel Vlase
Sweden	Mr. Thomas Lindstam
United Kingdom	Mr. Mark Pritchard
United Kingdom	Mr. Nadhim Zahawi
United Kingdom	Lord Parry Mitchell

Executive Reports

Office of the Director of National Intelligence:
Safeguarding the Personal Information of all People

Privacy and Civil Liberties Oversight Board:
Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act

International Participants

Members of Parliament

Albania	Ms.	Arta Dade
Austria	Mr.	Reinhold Lopatka
Austria	Mr.	Andreas Schieder
Austria	Dr.	Andreas Karlsboeck
Austria	Dr.	Peter Pilz
Austria	Ms.	Jessi Lintl
Austria	Mr.	Christoph Vavrik
Bosnia	Mr.	Saša Magazinović
Croatia	Mr.	Josip Leko
Croatia	Dr.	Miroslav Tuđman
Czech Republic	Mr.	Marek Ženíšek
Denmark	Ms.	Pernille Skipper
Denmark	Mr.	Karsten Nonbo
Estonia	Mr.	Marko Mihkelson
Finland	Ms.	Tuija Brax
Finland	Mr.	Jouni Laaksonen
Georgia	Mr.	Tedo Japaridze
Georgia	Mr.	Irakli Sesiashvili
Georgia	Mr.	Irakli Chikovani
Georgia	Mr.	Davit Darchiashvili
Georgia	Ms.	Tinatin Khidasheli
Germany	Mr.	Stephan Mayer
Germany	Ms.	Nina Warken
Germany	Dr.	Tim Ostermann
Germany	Ms.	Susanne Mittag
Germany	Mr.	Mahmut Özdemir
Germany	Ms.	Martina Renner
Germany	Mr.	Özcan Mutlu

Germany	Mr.	Christian Ströbele
Germany	Dr.	Patrick Sensburg
Greece	Mr.	Kostas Tsiaras
Greece	Mr.	Kostas Triantafyllos
Hungary	Mr.	Gergely Gulyás
Hungary	Mr.	Tamás Harangozó
Hungary	Dr.	András Schiffer
Hungary	Mr.	György Szilágyi
Hungary	Ms.	Katalin Csöbör
Hungary	Mr.	Mátyás Firtli
Ireland	Mr.	Pat Breen
Italy	Mr.	Paolo Gentiloni
Latvia	Mr.	Ainars Latkovskis
Lithuania	Mr.	Emanuelis Zingeris
Luxembourg	Mr.	Eugène Berger
Malta	Dr.	Anġlu Farrugia
Malta	Mr.	Carmelo Abela
Montenegro	Mr.	Ranko Krivokapić
Norway	Mr.	Kenneth Svendsen
Poland	Ms.	Beata Bublewicz
Poland	Mr.	Marek Wójcik
Poland	Mr.	Marek Opioła
Portugal	Mr.	Sérgio Sousa Pinto
Romania	Mr.	Valeriu Zgonea
Romania	Dr.	Gabriel Vlase
Sweden	Mr.	Ulf Holm
Sweden	Ms.	Eliza Rozstokowska Öberg
United Kingdom	Lord	Paul Boateng
United Kingdom	Lord	Parry Mitchell
United Kingdom	Mr.	Mark Hendrick
United Kingdom	Mr.	Nadhim Zahawi
United Kingdom	Mr.	Mark Pritchard

International Participants

Ambassadors

Georgia	His Excellency Archil Gegeshidze
Germany	His Excellency Peter Wittig
Latvia	His Excellency Andris Razāns
Montenegro	His Excellency Srđan Darmanović
Romania	His Excellency Iulian Buga
Serbia	His Excellency Vladimir Jovičić
Slovenia	His Excellency Božo Cerar
Sweden	His Excellency Björn Lyrvall