June 24, 2016

Dear Senator:

The undersigned civil society organizations, companies, trade associations and academics strongly oppose a provision of the Intelligence Authorization Act for FY 2017 (Act, S. 3017) that would bar the U.S. Privacy and Civil Liberties Oversight Board (PCLOB) from considering the privacy and civil liberties interests of anyone but citizens and lawful permanent residents of the U.S. (U.S. persons). We urge you to oppose any version of this legislation that includes this provision.

PCLOB plays an important role in protecting privacy and civil liberties in the counter-terrorism context. Congress created PCLOB in response to a recommendation of the 9/11 Commission, reinforced its independence in 2008, and has considered carefully the reform recommendations this expert body has made. In its report on Section 702 of the Foreign Intelligence Surveillance Act (FISA), PCLOB indicated that it planned to address the impact of surveillance on non-U.S. persons in its next report. That report is being prepared and will focus on electronic surveillance conducted under Executive Order 12333 directed largely outside the U.S. Section 603 would bar PCLOB from addressing the rights of non-U.S. persons in that report, even though the surveillance the report will consider has an enormous impact on non-U.S persons, as well as on U.S. persons.

The President recognized the important role that the PCLOB can and should play to protect the rights of people outside the United States in the surveillance context. Presidential Policy Directive 28 (PPD-28)[1] states:

> All persons should be treated with dignity and respect, regardless of their nationality or wherever they might reside, and all persons have legitimate privacy interests in the handling of their personal information.

It encouraged PCLOB to provide a report that assesses the implementation of PPD-28 that fall within PCLOB's mandate. Section 603 of the Act would limit PCLOB's mandate to protecting only the rights of U.S. persons, thus barring PCLOB from doing much of the review for which the President called.

Limiting PCLOB's authority in this way would also undermine the nascent Privacy Shield agreement, putting trans-Atlantic trade that is critical to the economy of the U.S. and Europe at greater risk. Privacy Shield – the proposed successor to the EU-US Safe Harbor Agreement – is designed to set privacy rules for data of EU residents transferred to and processed in the U.S. Regardless of one's view on the sufficiency of the Privacy Shield, the agreement was the product of extensive, delicate negotiations. It relies, in part, on assurances the U.S. made about PCLOB's role in overseeing the use of surveillance authorities that apply to non-U.S. persons, such as Section 702 of FISA.[2] EU regulators have specifically taken note of the report in progress on E.O. 12333. Section 603 would damage the ongoing diplomatic discussions with the EU by barring PCLOB from exercising oversight of the data of Europeans and other non-U.S. persons.

---

[1] https://www.whitehouse.gov/sites/default/files/docs/2014sigint_mem_ppd_rel.pdf.

[2] http://ec.europa.eu/justice/data-protection/files/privacy-shield-adequacy-decision-annex-6_en.pdf.

Section 603 would also bar PCLOB from considering the rights of non-U.S. persons even when they are inside the U.S. Both the Fourth Amendment to the U.S. Constitution and the Foreign Intelligence Surveillance Act protect everyone in the U.S. regardless of their citizenship: a court order, based on a showing that a person in the U.S. is an agent of a foreign power, is generally required to collect the contents of a person's communications in an intelligence investigation. But, for example, if a newspaper reported that the NSA was collecting the communications content of lawfully present foreign students, businesspersons, or other visitors to the U.S. without the required court order, Section 603 would bar PCLOB from investigating such a potential violation of the law, and the U.S. Constitution. Moreover, in cases where the impact of a program on U.S. persons is not immediately apparent, this limitation could complicate PCLOB's efforts to protect the rights of U.S. persons as well.

This provision is detrimental to human rights and to trans-Atlantic trade. A number of companies and civil society groups previously urged you to reject Section 803 of the Act, which would empower the FBI to issue National Security Letters that demand, without court authorization, disclosure of electronic communication transactional records held by communications service providers.[3] Signatories to this letter urge you to oppose any version of the Intelligence Authorization Act of FY 2017 that bars PCLOB from considering the rights of non-U.S. persons.

Sincerely,

Companies, trade associations, and civil society groups:
Access Now
Advocacy for Principled Action in Government
American-Arab Anti-Discrimination Committee
American Civil Liberties Union
Apple
Arab American Institute
Asociación por los Derechos Civiles (ADC), Argentina
Brennan Center for Justice
Center for Democracy & Technology
Change.org
Church World Service
Coalition for Humane Immigrant Rights of Los Angeles (CHIRLA)
Computer & Communications Industry Association (CCIA)
Constitution Project
Council on American-Islamic Relations
Fight for the Future
Global Network Initiative
Google
Government Accountability Project
Human Rights Watch
Immigrant Legal Resource Center
Intel

[3] https://www.aclu.org/letter/ectr-coalition-letter.

International Modern Media Institute, Reykjavik, Iceland
Internet Infrastructure Coalition / I2Coalition
Just Foreign Policy
Microsoft
National Korean American Service and Education Consortium (NAKASEC)
National Security Counselors
New America's Open Technology Institute
OpenMedia
Open Net Korea
PEN America
Reform Government Surveillance
Samuelson-Glushko Canadian Internet Policy & Public Interest Clinic (CIPPIC), Canada
Symantec
U.S. Committee for Refugees and Immigrants
United We Dream
Win Without War

Academics [Affiliations listed for purposes of identification only]:
Alvaro M. Bedoya, Georgetown Law, Center on Privacy and Technology
Michael W. Carroll, Professor of Law and Director, Program on Information Justice and Intellectual Property, American University Washington College of Law
Estelle Derclaye, Professor of Intellectual Property Law, University of Nottingham School of Law, United Kingdom
Susan Freiwald, Professor of Law, University of San Francisco School of Law
Roger Allan Ford, Assistant Professor of Law, University of New Hampshire School of Law
Michael Froomkin, University of Miami School of Law
Jennifer Stisa Grannick, Director of Civil Liberties, Stanford Center for Internet & Society
Vivek Krishnamurthy, Clinical Director – Cyberlaw Clinic, Harvard Law School / Berkman Center for Internet & Society
Molly K. Land, Professor of Law and Human Rights and Associate Director, Human Rights Institute
Mark A. Lemley, Professor, Stanford Law School
Paul K. Ohm, Professor, Georgetown University Law Center
K.S. Park, Professor, Korea University Law School
Chip Pitts, Professor, Stanford/Oxford
Charles Raab, Professorial Fellow, University of Edinburgh, Scotland, United Kingdom
Neil Richards, Professor of Law, Washington University
Ira Rubinstein, Senior Fellow, Information Law Institute, NYU School of Law
Pamela Samuelson, Professor of Law, Berkeley Law School, Director of the Berkeley Center for Law & Technology
Adina Schwartz, Professor, John Jay College of Criminal Justice, CUNY
Robert H. Sloan, Professor and Head of Dept. of Computer Science, University of Illinois at Chicago
Katherine Strandburg, Professor of Law, New York University School of Law
Peter Swire, Professor of Law and Ethics, Georgia Tech Scheller College of Business
Jennifer M. Urban, Clinical Professor of Law and Director, Samuelson Law, Technology & Public Policy Clinic, UC Berkeley School of Law