KEEPING THE INTERNET
OPEN • INNOVATIVE • FREE

www.cdt.org

CENTER FOR DEMOCRACY
& TECHNOLOGY

1634 I Street, NW
Suite 1100
Washington, DC 20006

P +1-202-637-9800
F +1-202-637-0968
E info@cdt.org

RE: WRITTEN STATEMENT REGARDING SHORT AND LONG TERM AGENDA OF THE PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD

August 29, 2014

Dear Ms. Franklin:

Thank you for the opportunity to make an oral statement on behalf of the Center for Democracy & Technology ("CDT") at the July 23 meeting of the Privacy and Civil Liberties Oversight Board ("PCLOB"). This written statement is submitted in connection with that meeting as prescribed in the July 9 Notice placed in the Federal Register, 79 Fed. Reg. 38999. CDT urges PCLOB, as part of its medium and long-term agenda, to examine and report upon the effect on privacy and civil liberties of:

- Surveillance conducted under Executive Order 12333 ("EO 12333");
- surveillance under all intelligence authorities on non-U.S. persons' rights to privacy, free expression and redress, including implementation of Presidential Policy Directive 28 ("PPD-28)";
- cybersecurity measures; and
- the activities of federal agencies at fusion centers.

We now briefly identify a non-exhaustive list of issues within each of these matters that the PCLOB examination should include.

Surveillance Under Executive Order 12333

Executive Order 12333 governs surveillance and other intelligence gathering activities, including human intelligence and signals intelligence directed outside the United States. Surveillance that targets U.S. persons (citizens and lawful permanent residents of the U.S.) abroad is conducted under the Foreign Intelligence Surveillance Act ("FISA") as opposed to EO 12333. EO 12333 was first issued in 1981. It was modified in 2003, 2004, and, most recently, in 2008 to accommodate creation of the Office of the Director of National Intelligence. Each intelligence agency issues regulations that interpret EO 12333, and for purposes of surveillance conducted under the Executive Order, DOD Regulation 5240.1-R (1982),[1] which governs DOD surveillance activities that could affect U.S. persons and the United States Signals Intelligence Directive, USSID-18 (2011)[2] are

[1] Available at, http://www.dtic.mil/whs/directives/corres/pdf/524001r.pdf.

[2] Available at, http://www.dni.gov/files/documents/1118/CLEANEDFinal%20USSID%20SP0018.pdf.

perhaps the most relevant for PCLOB's consideration.

EO 12333 is the legal grounding for mass surveillance activities, including many brought to public attention for the first time in documents released by Edward Snowden. Among other things, EO 12333 is the basis for bulk collection of:

> (i) location information generated by use of mobile devices;[3]
> (ii) communications content passing over the main communications links that connect data centers around the world, including Yahoo and Google data centers;[4]
> (iii) text messages;[5] and
> (iv) email address books.[6]

These collection activities sweep in communications of many U.S. persons even though U.S. persons are not targeted for surveillance. PCLOB's review should include an assessment as to whether EO 12333 and the regulations issued thereunder adequately protect U.S. persons' rights, and in particular, whether the minimization for which it calls is up to the task of protecting U.S. persons' rights, given the breadth of collection the Executive Order authorizes and the context in which it occurs. PCLOB should assess whether minimization procedures are an adequate protection for bulk collection activities that can reasonably be anticipated to sweep in a significant proportion of U.S. persons' communications. When, for example, the NSA can reasonably anticipate that a significant proportion of the communications seized by tapping the back-ups between data centers of a U.S. tech company will be those of U.S. persons, it collects those communications in bulk nonetheless. PCLOB should assess whether this is appropriate and whether, instead, additional protections are called for at collection when it is reasonable to believe that a significant portion of the collected data will include the communications of U.S. persons.

PCLOB should assess whether the scope of permissible intelligence surveillance under EO 12333 is overbroad. The Executive Order authorizes surveillance in order to collect "foreign intelligence," which is defined broadly to include the activities and intentions of any foreign individual or organization. This is not a meaningful limitation. For purposes of intelligence surveillance under the Executive Order, PCLOB should consider whether the much more

---

[3] *See, e.g.*, Barton Gellman and Ashkan Soltani, NSA tracking cellphone locations worldwide, Snowden Documents Show, *The Washington Post*, December 4, 2013, *available at* http://www.washingtonpost.com/world/national-security/nsa-tracking-cellphone-locations-worldwide-snowden-documents-show/2013/12/04/5492873a-5cf2-11e3-bc56-c6ca94801fac_story.html.

[4] *See, e.g.*, Barton Gellman and Ashkan Soltani, NSA infiltrates links to Yahoo, Google data centers worldwide, Snowden documents say, *The Washington* Post, October 30, 2013, *available at* http://www.washingtonpost.com/world/national-security/nsa-infiltrates-links-to-yahoo-google-data-centers-worldwide-snowden-documents-say/2013/10/30/e51d661e-4166-11e3-8b74-d89d714ca4dd_story.html.

[5] *See, e.g.*, James Gall, NSA collects millions of text messages daily in 'untargeted' global sweep, *The Guardian*, January 16, 2014, *available at* http://www.theguardian.com/world/2014/jan/16/nsa-collects-millions-text-messages-daily-untargeted-global-sweep.

[6] *See, e.g.*, Barton Gellman and Ashkan Soltani, NSA collects millions of e-mail address books globally, *The Washington Post,* October 14, 2013, *available at* http://www.washingtonpost.com/world/national-security/nsa-collects-millions-of-e-mail-address-books-globally/2013/10/14/8e58b5be-34f9-11e3-80c6-7e6dd8d22d8f_story.html.

restrictive definition of "foreign intelligence" that appears in FISA should be used instead.[7] Other types of intelligence activities under EO 12333 could be conducted under a broader definition of foreign intelligence.

Finally, Executive Order 12333 and regulations issued thereunder were secretly interpreted in 2007 to permit so-called "contact chaining." This is intelligence jargon for the compelled collection from U.S. providers of calling records and Internet transactional records of U.S. persons in the U.S. without a particularized court order, even though the applicable regulation explicitly prohibited such conduct. In other words, a secret interpretation of a regulation issued under EO 12333 reversed privacy protections in the public regulation issued under the Executive Order. PCLOB's review ought to include the identification and public disclosure of secret interpretations of public documents issued under the authority of EO 12333 that limit or reverse privacy protections in the public documents.

Rights of Non-U.S. Persons

PCLOB's agenda should also include a searching examination of the impact of U.S. surveillance activities under all intelligence authorities, including Executive Order 12333 and FISA Section 702, on the rights of non-U.S. persons to privacy, free expression and redress for violation of rights. PCLOB has already committed to examining the rights of non-U.S. persons in the context of the input it plans to offer on implementation of PPD-28. This is insufficient because PPD-28 is so limited. In particular, while PPD-28 does call for subjecting information about non-U.S. persons to the same *retention and dissemination* restrictions that pertain to information collected about U.S. persons, it does not subject *collection* activities to such restrictions. When assessing the impact of surveillance on the rights of non-U.S. persons, we urge you to assess collection activities as well.

PCLOB's assessment of the rights of non-U.S. persons ought to start with internationally accepted human rights. Indeed, PPD-28 states that non-U.S. persons have such rights, but does little to spell them out. Last year, CDT released a report that includes a normative framework based on human rights standards that can be used for assessing surveillance activities.[8] This year, the United Nations High Commissioner for Human Rights issued a report that also provides an excellent framework for analyzing U.S. surveillance activities under international law.[9] In addition, hundreds of civil society groups around the country, including CDT, have endorsed the "Necessary and Proportionate Principles,[10] which could also serve as a starting point for PCLOB's assessment. In making its assessment, we urge the PCLOB to focus in particular on the internationally recognized rights to privacy, free, expression, and the right to a remedy for violations of these rights.

---

[7] CDT believes the FISA definition of "foreign intelligence" at 50 USC 1801 is also overbroad, but it is significantly narrower than the definition in EO 12333.

[8] CDT Releases Report on Governments' Systematic Access to Personal Data, *The Center for Democracy and Technology* (November 20, 2013), *available at* https://cdt.org/press/cdt-releases-report-on-governments'-systematic-access-to-personal-data/.

[9] The report can be found here: http://www.ohchr.org/EN/AboutUs/Pages/WhoWeAre.aspx. CDT's analysis of the report is here: https://cdt.org/blog/major-un-privacy-report-is-a-strong-blow-against-us-surveillance-regimes/.

[10] Available at, https://en.necessaryandproportionate.org/text.

Cybersecurity

We also urge PCLOB to interpret its statutory mandate to include an assessment of the civil liberties implications of cybersecurity measures, both those in place today, and those that are being contemplated. The measures include the sharing of cybersecurity threat information gleaned from users' Internet communications, countermeasures and "active defense" activities that can destroy data or make it inaccessible to users, botnet takedowns, which can sometimes render websites of those other than the wrongdoer inaccessible to the public, and the policies around governmental stockpiling of "zero day" vulnerabilities. Zero day vulnerabilities are those that have not previously been disclosed to maker of the software that has the vulnerability. The NSA can use zero days to exploit communications. However, the stockpiling of zero day vulnerabilities leaves Internet communications less secure, because hackers and other wrongdoers can discover and exploit the vulnerability as well.

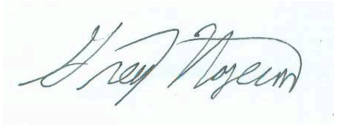
Fusion Centers

Finally, we urge PCLOB to examine the activities of federal agencies at the intelligence fusion centers that operate around the country. Fusion centers are designed to bring together federal, state, local and tribal law enforcement agencies to exchange information about terrorist threats. The mission of fusion centers has, however, expanded significantly beyond terrorism. A number of media reports have indicated that information gathered and then shared at fusion centers is information protected by the First Amendment to the U.S. Constitution. The functional standard for collecting threat information that is exchanged at fusion centers may need to be strengthened. Moreover, fusion centers can be used by a law enforcement agency that operates under privacy protective guidelines to obtain from another law enforcement agency the very information that its protective guidelines bar it from collecting itself. An examination by PCLOB of the activities of federal agencies at fusion centers could help ensure that they operate in a manner consistent with privacy and civil liberties.

Conclusion

Thank you for providing us with this opportunity to share our views about programs and activities that PCLOB ought to assess in the medium and long term.

Sincerely,



Gregory T. Nojeim
Director, Freedom, Security & Technology Project