



PRIVACY & CIVIL LIBERTIES OVERSIGHT BOARD

MEETING SUMMARY

Topic: Board meeting with NGOs on E.O. 12333
Date: Dec. 17, 2014
Location: 2000 M St. NW, Washington, D.C.

PCLOB Participants: Board Members
Sharon Bradford Franklin
E.O. 12333 Team

Participating Individuals and Organizations:

Alvaro Bedoya, Georgetown University Center on Privacy and Technology
Hannah Bloch-Wehba, Reporters Committee for Freedom of the Press
William Burgess, Council on American-Islamic Relations (by phone)
Shahid Buttar, Bill of Rights Defense Committee
Laura Donohue, Georgetown University
Patrick Eddington, Cato Institute
Laura Gaurav, Government Accountability Project
Robyn Greene, Open Technology Institute at the New America Foundation
Neema Singh Guliani, ACLU
Katherine Hawkins, OpentheGovernment.org
Robert McCaw, Council on American-Islamic Relations
Kel McClanahan, National Security Counselors
Patrice McDermott, OpenTheGovernment.org
Drew Mitnick, Access
Jumana Musa, National Association of Criminal Defense Lawyers
Greg Nojeim, Center for Democracy & Technology
Joe Onek, The Raben Group
Faiza Patel, Brennan Center for Justice
Yolanda C. Rondon, American-Arab Anti-Discrimination Committee
Julian Sanchez, Cato Institute
Jeramie Scott, Electronic Privacy Information Center
Rita Siemion, The Constitution Project
Amos Toh, Brennan Center for Justice (by phone)

Sean Vitka, Sunlight Foundation (by phone)
Nathan White, Demand Progress
Cynthia Wong, Human Rights Watch

I. Background

On December 17, 2014, the PCLOB convened a meeting to better understand public concerns about Intelligence Community (“IC”) activities conducted under Executive Order 12333. The PCLOB invited representatives from a range of organizations, including advocacy groups, policy institutes, and academic institutes, to present their views and questions to Board members and staff. The following summary organizes, thematically and topically, the questions and suggestions raised at the meeting.

II. Summary

A. Suggested Frameworks for 12333 Analysis

Participants proposed the following possible frameworks for the PCLOB’s analysis of E.O. 12333 activities:

- *Laura Donohue (Georgetown University)* suggested that the PCLOB consider, at a broad level, (1) the scope of activities conducted under the auspices of E.O. 12333, including domestic activities; (2) how information is being used; and (3) separation of powers issues. She also offered the following more detailed rubric:
 1. Definitions
 - a. What falls outside FISA?
 - b. What falls inside 12333?
 2. Analysis of the amendments to the E.O. and their significance
 3. How is the information being used (process, architecture, substance)?
 - a. What kind of stored versus in-transit information is collected?
 - b. What kind of communication-related data (buddy lists, address lists, etc.) is collected?
 - c. Does 12333 collection reach social network sites, voicemail, cookies, public billboards, etc.?
 4. Analysis of how information is used, particularly in the criminal sphere (noting that PCLOB’s 702 report did not address the Fourth Amendment reasonableness of FBI queries performed in criminal cases).
 5. Separation of powers analysis that might reference some of the following:
 - a. Declassified Office of Legal Counsel memos quoted by Sen. Whitehouse regarding the proposition that a president can depart from executive orders at any point;
 - b. The boundaries of Congress’s sphere of influence on executive branch intelligence-gathering activities;
 - c. How to think about the problem and potential solutions:

- i. Do we need improved oversight?
 - ii. More delineated authorities?
- 6. An analysis of legal protections in other countries (the United Kingdom has 8 protections that the United States does not)
- *Julian Sanchez (Cato Institute)* suggested that the PCLOB:
 - Consider the technical modes of collection (the “architectures” of collection) as much as it considers the rules about when and how these methods can be used (noting that the installation of a microphone in every home is different from the rules about when it can be turned on); and
 - Focus on the interplay between 12333 collection and domestic authorities and, in particular, (a) the extent to which the option of “back door” collection under 12333 undermines requirements of “front end” access; and (b) the use of “bulky” collection overseas to develop targets for what then appears to be targeted collection under domestic authorities.
- Several participants urged that the PCLOB engage in a constitutional analysis of the following topics:
 - The outer bounds of the president’s Article II authority and the limits of Congress’s authority to issue legislation that affects executive branch intelligence activities.
 - The extent to which E.O. 12333 activities circumvent Fourth Amendment protections.
- Some participants asked whether the IC conducts a human rights assessment of its collection, use, and dissemination activities. They raised the following points:
 - The primary sources of relevant rights under international law are the International Covenant on Civil and Political Rights (“ICCPR”) and the American Declaration on Human Rights.
 - Under international human rights law, interference with privacy must be lawful and non-arbitrary. There is concern that collection under E.O. 12333, to the extent that is indiscriminate, is arbitrary.
 - Collection/acquisition (as understood in plain language) is not innocuous, and can itself interfere with human rights and privacy, apart from use.
 - International human rights law provides a right to a remedy, but it is difficult to identify the individual(s) to whom remedies are due.
 - The U.S. government takes the position that U.S. privacy protections don’t apply extraterritorially. This raises concerns from a comity perspective — does the U.S. position provide incentives for other countries to engage in collection activities on a similar scale within the United States?
 - It is important to conduct a human rights assessment of IC decisions to share information with foreign governments.

B. The Relationship Between the PCLOB's E.O. 12333 Analysis and its PPD-28 Analysis

Some participants raised the following questions about how the PCLOB's assessment of PPD-28 implementation might relate to its 12333 analysis:

- Is it possible to write an E.O. 12333 report while an assessment of PPD-28 implementation is still ongoing?
- How is PPD-28's requirement that agencies conduct their SIGINT activities in a manner that is as narrowly tailored as feasible being implemented in the context of 12333 collection?

C. The Public's Ability to Engage with Board Reports on E.O. 12333

One participant (*Katherine Hawkins, OpenTheGovernment.org*) raised the following questions and concerns about whether the public would be able to react to the Board's factual findings in a manner that could meaningfully influence public discourse and even the Board's own analysis:

- Generally, there is not enough information available to allow for public participation in debates on E.O. 12333.
- Once the Board's report is issued and its conclusions have been drawn, it might be too late for the public to meaningfully influence debate.
- In that light, is it possible for the PCLOB to make some meaningful disclosures to the public before it issues a formal report?

D. The Scope and Contents of Intelligence Agencies' Collection Under E.O. 12333

Meeting participants were heavily focused on the overall scope of E.O. 12333 collection, including the scope of bulk or non-targeted collection and the scope of incidental collection of U.S. person information. This topic was emphasized by nearly all participants. Some participants noted that the scope of collection against non-U.S. persons was also of interest. Others expressed concern that E.O. 12333 permits intelligence agencies to broadly construe a foreign intelligence purpose to justify collection.

Key questions/comments:

- What is the "Golden Number" of USP communications incidentally collected?¹ Some participants viewed answering this question as a prerequisite for posing additional questions and offering analysis, "because it tells us how much we should be worried" (*Nathan White, Demand Progress*).
- The Board might consult mathematicians and engineers about how to design a survey that could produce the Golden Number and whether such a survey could be conducted without human review of communications.

¹ See Alvaro Bedoya, *Executive Order 12333 and the Golden Number*, JUST SECURITY (Oct. 9, 2014), <http://justsecurity.org/16157/executive-order-12333-golden-number/>.

- What is the scope of collection against foreign persons?
- How does the number of communications collected compare to what is collected under Section 702?
- What is the breakdown of 12333 collection between targeted and bulk activities?
 - How “bulky” does overseas collection get (e.g., “everyone speaking Pashto in Germany”)? (*Julian Sanchez, Cato Institute*)
- How broadly is the foreign intelligence purpose construed?
 - “It’s hard to imagine when you couldn’t collect on a foreign person [based on the E.O.’s definition of foreign intelligence]. Is it not this broad?” (*Cynthia Wong, Human Rights Watch*)
- To what extent are our own collection rules undermined by sharing with countries that are not governed by our rules (i.e., concern about “wink and nod” sharing of information on USPs) (*Greg Nojeim, Center for Democracy & Technology*)
- The Board should assess the propriety of collecting information in bulk in light of the fact that it is reasonable to believe that this form of collection will sweep up a significant number of USPs.
- The Board should consider ways to narrow permissible surveillance targets to legitimate interest — something more like FISA’s “agent of a foreign power.”
- The Board should consider the cybersecurity implications of certain 12333 activities, e.g. undermining encryption standards and stockpiling vulnerabilities.
- The Board should examine the rules on collection of attorney-client communications.
- The Board should release the number of Arabs/Arab-Americans subject to monitoring. (*Yolanda Rondon, American-Arab Anti-Discrimination Committee*)
- Participants also raised the following questions about the commercial impact of E.O. 12333 collection:
 - Is data held by American companies more or less secure than data held by foreign companies?
 - Is the answer to this question likely to reduce foreigners’ demand for U.S. products?
 - If data held on U.S. servers is mirrored elsewhere, are IC agencies legally obligated to first seek the information on U.S. servers?

E. Use and Dissemination of Information Collected Under E.O. 12333

Participants were generally interested in obtaining more information about how data collected pursuant to E.O. 12333 is used and disseminated, both to other U.S. federal and states agencies, and to foreign governments.

Key questions/comments:

- How is information collected pursuant to E.O. 12333 used in federal criminal proceedings, and in federal civil or regulatory matters like watchlists and immigration proceedings?

- What is the extent to which law enforcement agencies may rely on this information to engage in “parallel construction”?
- To what extent does the IC disseminate information about non-targeted individuals?
- Does the IC conduct a human rights assessment prior to sharing information with foreign governments?
- How does the United States audit or assess how other countries use information received from the United States?

F. Retention of Information Collected Under 12333

Participants were also interested in understanding the rules governing the retention of information and PCLOB’s assessment of the consistency and adequacy of these rules.

Key questions/comments:

- PCLOB should provide an understanding of the minimization procedures that agencies apply.
- How do these minimization procedures deviate from those under FAA Section 702?
- Does the United States apply minimization procedures to information received from other countries or voluntarily provided by companies?
- How is it possible to achieve consistency if each agency has its own minimization procedures? Should there be uniformity?
- Please evaluate the effectiveness and/or adequacy of minimization procedures.
- Is after-the-fact minimization good enough to protect both USPs and non-USPs? Consider additional limitations on the scope of collection.

G. Evaluation of Oversight Mechanisms

Several participants recommended that the PCLOB assess the operation and adequacy of existing oversight mechanisms.

Key questions/comments:

- “Who are the decision makers? Who else balances [the costs and benefits of 12333 activities] besides the IC?”
- How can Congress improve its oversight?
- Can there be FISC-analogous judicial oversight of E.O. 12333 activities?
- Are there too many oversight mechanisms in place? If so, does this result in a situation where no particular body takes responsibility for oversight?

H. Transparency

Participants raised the following suggestions about how the Board might promote transparency:

- The PCLOB should make its report and recommendations public.
- The Board should catalog the information that is declassified as a result of its investigation.
- The Board should push for declassification of the legal bases for 12333 surveillance and how the government is interpreting the rules (example: the contact-chaining SPCMA memo seemed contrary to natural reading of E.O. 12333 guideline). “Tell us about the important interpretations.” (*Greg Nojeim, CDT*)
- The Board might consider whether it wishes to become a contact point for whistleblowers and thus promote transparency. (*Laura Gaurav, Government Accountability Project*)