



June 16, 2015

Privacy and Civil Liberties Oversight Board
2100 K St. NW, Suite 500
Washington, D.C. 20427

Re: Request for Public Comment on Activities under Executive Order 12333

Dear Chairman Medine and Board Members:

The Constitution Project is a non-profit think tank and advocacy organization that brings together unlikely allies—experts and practitioners from across the political spectrum—to develop consensus-based recommendations to some of the most difficult constitutional challenges of our time. We conduct strategic public education campaigns and advocacy efforts to further these legal and policy recommendations. Through our Liberty and Security Committee, which was created in the aftermath of the 9/11 attacks, The Constitution Project works to ensure that our nation protects both our national security and our civil liberties. As part of these efforts, TCP has long advocated in favor of an independent Privacy and Civil Liberties Oversight Board with meaningful oversight authority over counterterrorism policies and programs to ensure that they incorporate robust safeguards for privacy and civil liberties.

The Constitution Project welcomes this opportunity to comment regarding the Board's inquiry into counterterrorism activities conducted under Executive Order (E.O.) 12333 and whether those activities properly balance efforts to protect the nation with privacy and civil liberties. In this regard, we urge the Board to review those activities, both during this initial inquiry and going forward, not simply for compliance with existing constitutional doctrines, laws, regulations, guidelines, and policies. The Board's primary mandate is to assess whether those activities strike an appropriate balance between liberty and security. By definition, such an assessment must involve an analysis of the efficacy of such activities in preventing acts of terrorism.

E.O. 12333, which was issued by President Ronald Reagan in 1981, is the comprehensive regulatory framework that established the capacities and powers of the different intelligence agencies,¹ including the NSA's signals intelligence collection abroad.² The activities conducted under E.O. 12333, most of which are unknown to the public, raise significant constitutional questions. These comments highlight some of those questions in five areas: separation of powers,

¹ See Exec. Order No. 12,333, 3 C.F.R. 200 (1981); see also Ellen Nakashima & Ashkan Soltani, *Privacy Watchdog's Next Target: The Least-Known but Biggest Aspect of NSA Surveillance*, WASH. POST, July 23, 2014, available at <http://www.washingtonpost.com/blogs/the-switch/wp/2014/07/23/privacy-watchdogs-next-target-the-least-known-but-biggest-aspect-of-nsa-surveillance/>.

² See Alvaro Bedoya, *Executive Order 12333 and the Golden Number*, JUST SECURITY, Oct. 9, 2014, available at <http://justsecurity.org/16157/executive-order-12333-golden-number/>.

checks and balances, transparency, Fourth Amendment protections, and First Amendment protections. This is not to suggest that this Board could or should answer these difficult constitutional questions. But it can conduct its inquiry into E.O. 12333 activities with an eye toward these questions so that in its public report on the framework established by E.O.12333, the Board can provide sufficient information to enable a public discussion of these issues.

Separation of Powers and the Limits of Article II Authority

E.O. 12333 is not itself a source of authority. As noted above, the order sets forth an organizational framework for the intelligence community's activities. The authority for those activities comes from statutes passed by Congress or from Article II executive power. The Board's current inquiry is presumably focused on the latter, and appropriately so. But while the executive branch undoubtedly has some inherent authority under Article II to conduct electronic surveillance to obtain communications from those "who plot unlawful acts against the Government," this executive authority is not unlimited.³ The precise scope and limits of inherent executive authority in this realm remain unsettled, particularly in the context of mass surveillance enabled by rapidly changing technological capabilities. Current law is also unsettled as to the extent executive power in this sphere precludes Congressional regulation.⁴ With Congress, the courts, and the public largely in the dark regarding the full extent of intelligence activities conducted under E.O. 12333, it is difficult to assess whether the inherent authority the executive branch is currently asserting comports with our constitutional system of both enumerated and separated powers. Such questions are worth the Board's attention.

Checks and Balances

There is a marked absence of external checks by the other two branches of government with respect to E.O. 12333 activities. While there are safeguards, or "checks," in place with respect to E.O. 12333 activities, including in the order itself and in PPD-28, those checks are primarily internal to the executive branch. This scenario raises questions about whether the existing checks sufficiently cabin the power of the executive branch,⁵ and to what extent the absence of external checks becomes increasingly problematic as technological capabilities continue to advance.

With respect to congressional oversight, reports indicate that even the intelligence oversight committees are in the dark regarding E.O. 12333 activities.⁶ Sen. Dianne Feinstein, Vice Chairman

³ See *United States v. U.S. Dist. Court*, 407 U.S. 297, 310 (1972); see also Deborah N. Pearlstein. Prepared Testimony to the Privacy & Civil Liberties Oversight Board. Public Meeting on Executive Order 123333. May 13, 2015.

⁴ See Deborah N. Pearlstein. Prepared Testimony to the Privacy & Civil Liberties Oversight Board. Public Meeting on Executive Order 123333. May 13, 2015 ("The activities regulated by E.O. 12333 generally avoid the structure of multi-branch participation the Constitution presumes is best suited to protecting individual rights, for example; here, executive agencies make the rules, the attorney general approves them, agencies then implement them – with no legislative authorization or other politically transparent rulemaking process in the first instance, and no judicial review or other reigours, independent check after the fact.").

⁶ See John Napier Tye. *Meet Executive Order 12333: The Regan rule that lets the NSA spy on Americans*, WASH. POST, July 18, 2014; see Deborah N. Pearlstein. Prepared Testimony to the Privacy & Civil Liberties Oversight Board. Public Meeting on Executive Order 123333. May 13, 2015. 1200 18th Street NW, Suite 1000, Washington, DC 20036 ☎ tel 202-580-6920 ☎ fax 202-580-6929 ☎ www.constitutionproject.org

of the Senate Intelligence Committee, has stated that the committee has not been able to sufficiently oversee the programs under E.O. 12333 and that such programs “are under the executive branch entirely.”⁷

There is also little to no judicial review of 12333 activities. Unlike intelligence collection and surveillance authorized by statute, no warrant or court approval is obtained before the executive branch collects communications, including the content of communications, under E.O. 12333.⁸

To what extent does the lack of congressional oversight or judicial review of these activities contribute to improper balancing of security and liberty? To what extent is the absence of checks by the coordinate branches of government constitutionally problematic?

Transparency

While some intelligence programs, methods, and capabilities undoubtedly must remain secret to be effective, secret *law* has no place in a democracy and some statistics on the privacy and civil liberties impact of even secret programs should be reported. Secret law operates in direct violation of the core constitutional principles of government by the people and separation of powers. The president committed to increased transparency and oversight of foreign intelligence surveillance activities, both in PPD-28 and in the December 2013 Open Government Partnership National Action Plan. The operation of secret law to justify secret programs belies the president’s commitments. This Board has an important role to play with respect to helping the public understand the scope of the legal authorities claimed by the executive branch under Article II and carried out under E.O. 12333.

As the exposure of the Section 215 telephony metadata program has demonstrated, Congress, the courts, and the public were unable to provide adequate checks on the executive without revelation of the program and its purported legal basis. It should not have taken a leak of classified information for the public to learn how the government had been interpreting Section 215 of the Patriot Act. The executive branch’s interpretation of the law, including its inherent Article II authorities to collect intelligence, interpretations of E.O. 12333, and related Office of Legal Counsel opinions, should be public. Meaningful public debate and rigorous oversight of government actions require transparency with respect to the legal rules and standards under which our government operates.

As The Constitution Project Liberty and Security Committee explained in its report examining the problem of secret law in the context of the targeted killing program:

Meeting on Executive Order 123333. May 13, 2015 (“[E]xecutive practice under 12333 was-and remains-little understood, even to members of congress.”).

⁷ See Ali Watkins. *Most of NSA’s data collection authorized by order Ronald Reagan issued*, MCCLATCHY DC, (Nov. 21, 2013), available at <http://www.mcclatchydc.com/2013/11/21/209167/most-of-nsas-data-collection-authorized.html>.

⁸ See John Napier Tye. *Meet Executive Order 12333: The Regan rule that lets the NSA spy on Americans*, WASH. POST, July 18, 2014, available at http://www.washingtonpost.com/opinions/meet-executive-order-12333-the-reagan-rule-that-lets-the-nsa-spy-on-americans/2014/07/18/93d2ac22-0b93-11e4-b8e5-d0de80767fc2_story.html.

The legal rules and standards under which our government operates should not be secret. While counterterrorism tactics and military strategy may be appropriately withheld from public disclosure, the public has a right to know the legal framework within which these and other operations are conducted, including the safeguards in place to protect constitutional and legal rights. While the president must be able to obtain frank and confidential legal advice about how the law may apply in particular circumstances, the governing rules themselves can never be secret . . .

Our constitutional system of checks and balances demands robust oversight by Congress and consideration and debate by an informed public. Neither is possible when the rules are hidden from Congress and from public view. Sensitive operational and intelligence details may of course remain appropriately classified. But the regime of law and applicable rules that govern national security programs must be made public. Our government's commitment to transparency must not evaporate the moment that national security concerns are invoked.⁹

This analysis applies similarly to government surveillance programs. The need for transparency regarding interpretations of the law is particularly strong where such interpretations are used as the legal basis for surveillance programs that remain secret. We urge the PCLOB to seek public interest declassification, with redactions only as necessary, of all legal opinions, memoranda, or orders regarding the legal authority for activities conducted under E.O. 12333.

The Board should also recommend statistical reporting to Congress and the public regarding the privacy and civil liberties impact and efficacy of activities conducted under E.O. 12333 in protecting the nation from terrorism. Examples of information the Board should recommend reporting on include:

- Analysis of the efficacy of programs conducted under E.O. 12333 in protecting the nation from terrorism. Information on efficacy is necessary for assessing the extent to which the need for the programs justifies any burdens on civil liberties and privacy.
- Information on the effectiveness of the government's minimization procedures in protecting the data of U.S. persons from warrantless review.
- The extent and scope of interceptions of the communications of U.S. persons and individuals located within the United States.
- The total number of targets and non-targeted persons affected by 12333 programs.
- Aggregate statistics on the number of intercepted communications in total.
- The number of intercepted communications to or from the United States or involving any U.S. person.
- An analysis of the performance of the government's targeting and minimization procedures.

⁹ Lift the Veil of Secrecy on Targeted Killing <http://www.constitutionproject.org/wp-content/uploads/2013/02/Lift-the-Veil-of-Secrecy-on-Targeted-Killing.pdf>

- An explanation of how collected information has been used, including the number of times the information has been used for law enforcement rather than foreign intelligence purposes.
- Statistic on the extent to which data collected under E.O. 12333 programs retained, searched, shared, and used.

This information should be provided in an unclassified form to the public, while more detailed information in classified form can and should be reported to Congress. Additionally, as much as practicable, other information on activities conducted under E.O. 12333 necessary for public understanding of the scope of surveillance authorities, the impact on privacy and civil liberties, and the historical development of the law should be released to the public, redacted as necessary.

Fourth Amendment

The Board should examine the extent to which Fourth Amendment protections rooted in assumptions about territoriality no longer reflect reality in the digital age in which communications may travel and/or be stored abroad even if the user never leaves home. The Board should assess whether Fourth Amendment doctrines developed in the pre-digital age are now enabling end-runs around constitutional protections.

E.O. 12333 authorizes the collection of the contents of a U.S. person's communications if those communications are "incidentally" collected during the course of a lawful overseas foreign intelligence investigation.¹⁰ Unlike surveillance within the borders of the United States or intelligence gathering activities that target U.S. citizens and legal residents, collection and retention of information under E.O. 12333 does not require a warrant.¹¹ Information on U.S. persons' can thus be collected without any suspicion of wrongdoing if it is stored or transmitted overseas,¹² as is increasingly the case.¹³ Bulk collection is allowed under E.O. 12333 to gather communications from American companies, which can store or "mirror" domestic communications on servers located overseas.¹⁴ The Executive Order does not require that companies be notified or give consent before users' communications are collected.¹⁵ E.O. 12333 does not prevent the collection and

¹⁰ See Exec. Order No. 12,333, 3 C.F.R. § 2.3(c); see also Ellen Nakashima & Ashkan Soltani, *supra*, n.1.

¹¹ See John Napier Tye, *Meet Executive Order 12333: The Regan rule that lets the NSA spy on Americans*, WASH. POST, (July 18, 2014), available at http://www.washingtonpost.com/opinions/meet-executive-order-12333-the-regan-rule-that-lets-the-nsa-spy-on-americans/2014/07/18/93d2ac22-0b93-11e4-b8e5-d0de80767fc2_story.html.

¹² See *id.*

¹³ See Barton Gellman & Ashkan Soltani, *NSA infiltrates links to Yahoo, Google data centers worldwide, Snowden documents say*, WASH. POST, (Oct. 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.

¹⁴ See Ellen Nakashima & Ashkan Soltani, *Privacy Watchdog's Next Target: The Least-Known but Biggest Aspect of NSA Surveillance*, WASH. POST, July 23, 2014; see also See Alvaro Bedoya, *Executive Order 12333 and the Golden Number*, JUST SECURITY, Oct. 9, 2014.

¹⁵ See John Napier Tye, *Meet Executive Order 12333: The Regan rule that lets the NSA spy on Americans*, WASH. POST, July 18, 2014.

retention of all such communications as long as the collection occurs overseas during the course of a lawful foreign intelligence or counterintelligence investigation.¹⁶

Moreover, there are no restraints on the volume of communications by U.S. persons that may be retained.¹⁷ Indeed, it is unknown how many Americans' communications are collected under 12333.¹⁸ The NSA has never released an estimate of how many Americans have had their communications collected under 12333.¹⁹ The scale of communications collected under E.O. 12333 is likely far greater than the collection under Section 702 of the Foreign Intelligence Surveillance Act (FISA).²⁰ E.O. 12333 allows for bulk collection of overseas electronic communications because there is no requirement that electronic surveillance be targeted at a specific individual.²¹ There is a substantial risk that bulk collection activities under 12333 are capturing U.S. persons' communications that are unrelated to foreign intelligence.²²

The Board should assess whether the bulk collection of U.S. persons' communications during the course of foreign intelligence investigations renders E.O. 12333 collection unreasonable under the Fourth Amendment. The Board should also examine whether the list of permissible collection purposes under E.O. 12333 should be narrowed. When targeting foreseeably involves collection of U.S. person data, the government should collect only intelligence related to the most severe national security risks. The Board should also assess the adequacy of data retention practices for information and communications collected under E.O. 12333, particularly information pertaining to U.S. persons or involving their communications.

The Board should also assess the scope of existing repositories of bulk metadata collected on U.S. persons under E.O. 12333 and whether or how the government should be permitted to use the bulk metadata already collected.²³ Relatedly, the Board should assess government data mining programs under E.O. 12333. While data mining may be able to provide a valuable investigative tool in certain situations, the benefits are unclear due to the difficulties of developing a predictive model or algorithm to identify terrorist suspects.²⁴ Data mining activities under E.O. 12333 also pose a

¹⁶ See Ellen Nakashima & Ashkan Soltani, *Privacy Watchdog's Next Target: The Least-Known but Biggest Aspect of NSA Surveillance*, WASH. POST, July 23, 2014; see also See Alvaro Bedoya, *Executive Order 12333 and the Golden Number*, JUST SECURITY, Oct. 9, 2014.

¹⁷ See John Napier Tye, *Meet Executive Order 12333: The Regan rule that lets the NSA spy on Americans*, WASH. POST, July 18, 2014.

¹⁸ See Alvaro Bedoya, *Executive Order 12333 and the Golden Number*, JUST SECURITY, Oct. 9, 2014.

¹⁹ See *id.*

²⁰ See *id.*

²¹ See *id.*

²² See *id.*

²³ *Coalition Letter Welcomes Privacy and Civil Liberties Oversight Board's Review of NSA Surveillance Programs*, (July 8, 2013), available at <http://www.constitutionproject.org/wp-content/uploads/2013/07/Coalition-ltr-to-PCLOB-on-NSA-program-7-8-13.pdf>.

²⁴ Statement of the Constitution Project Submitted to the Privacy and Civil Liberties Oversight Board, (Oct. 31, 2012), available at http://www.constitutionproject.org/wp-content/uploads/2012/10/103112_statementtopclob.pdf; see also The Constitution Project, *Principles for Government Data Mining: Preserving Civil Liberties in the Information Age* (2010), available at <http://www.constitutionproject.org/pdf/DataMiningPublication.pdf>.

threat to Americans' privacy rights and civil liberties due to the risks of "false positives."²⁵ In addition, the Board should evaluate whether the use of E.O. 12333-derived information obtained without a warrant in *any* proceeding against a U.S. person complies with the Fourth Amendment and other constitutional rights.

First Amendment

First Amendment rights are also implicated by intelligence collection under E.O. 12333. Bulk collection of communications content and metadata can have a chilling effect on free speech and may infringe upon the right to freely associate.²⁶ Where the collected data is later mined, particularly for determining associational relationships, the impact on First Amendment rights can be even more substantial. The Board should assess whether activities conducted under E.O. 12333 have sufficient safeguards against such infringement.

Thank you for the opportunity to submit these comments. The Constitution Project looks forward to continued engagement with the Board as it conducts its initial inquiry into activities governed by E.O. 12333.

Respectfully submitted,

Rita Siemion
Senior Counsel
The Constitution Project

²⁵ Statement of the Constitution Project Submitted to the Privacy and Civil Liberties Oversight Board, (Oct. 31, 2012), available at http://www.constitutionproject.org/wp-content/uploads/2012/10/103112_statementtopclob.pdf; see also The Constitution Project, Principles for Government Data Mining; Preserving Civil Liberties in the Information Age (2010), available at <http://www.constitutionproject.org/pdf/DataMiningPublication.pdf>.

²⁶ See The Constitution Project, Principles for Government Data Mining; Preserving Civil Liberties in the Information Age 14-15 (2010), available at <http://www.constitutionproject.org/pdf/DataMiningPublication.pdf>.