



August 29, 2014

Privacy and Civil Liberties Oversight Board
General Services Administration
c/o Ms. Flowers
Regulatory Secretariat Division (MVCB)
1800 F Street NW
Washington, DC 20405.

Re: Notice PCLOB 2014-04, Sunshine Act Meeting

AMERICAN CIVIL
LIBERTIES UNION
WASHINGTON
LEGISLATIVE OFFICE
915 15th STREET, NW, 6TH FL
WASHINGTON, DC 20005
T/202.544.1681
F/202.546.0738
WWW.ACLU.ORG

LAURA W. MURPHY
DIRECTOR

NATIONAL OFFICE
125 BROAD STREET, 18TH FL.
NEW YORK, NY 10004-2400
T/212.549.2500

OFFICERS AND DIRECTORS
SUSAN N. HERMAN
PRESIDENT

ANTHONY D. ROMERO
EXECUTIVE DIRECTOR

ROBERT REMAR
TREASURER

Dear Privacy and Civil Liberties Oversight Board Members:

Thank you for the opportunity to provide the American Civil Liberties Union's¹ views regarding the issues the Privacy and Civil Liberties Oversight Board (PCLOB) should include in its forthcoming agenda.

Many new and existing national security programs and authorities threaten privacy, civil liberties, and human rights. The items below represent areas where a full investigation by the PCLOB is urgently needed to inform future reforms, shed light on concerning practices, and provide meaningful oversight.

1. Executive Order 12333

Executive Order 12333 provides broad latitude for the government to conduct surveillance on U.S. and non-U.S. persons without judicial review or many other protections that would apply to analogous activities conducted under existing statutory authorities.² Little information is publicly available regarding the rules that apply to surveillance under Executive Order 12333 or the government's

¹ For nearly 100 years, the ACLU has been our nation's guardian of liberty, working in courts, legislatures, and communities to defend and preserve the individual rights and liberties that the Constitution and the laws of the United States guarantee everyone in this country. The ACLU takes up the toughest civil liberties cases and issues to defend all people from government abuse and overreach. With more than a million members, activists, and supporters, the ACLU is a nationwide organization that fights tirelessly in all 50 states, Puerto Rico, and Washington, D.C., for the principle that every individual's rights must be protected equally under the law, regardless of race, religion, gender, sexual orientation, disability, or national origin.

² John Napier Tye, *Meet Executive Order 12333: The Reagan Rule That Lets the NSA Spy on Americans*, WASHINGTON POST (July 18, 2014), 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.

practices under it. Recent disclosures suggest, however, that the NSA is sweeping up vast amounts of data worldwide under the order. For example, reports state that, pursuant to the order, the NSA collects nearly 5 billion records per day on the location of cell phones, including Americans' cell phones; hundreds of millions of contact lists or address books from personal email and instant messaging accounts; and information from Google and Yahoo user accounts as that information travels between those companies' data centers located abroad.³ This information is then retained and disseminated purely at the discretion of the executive branch, without oversight by the Foreign Intelligence Surveillance Court or another independent body. Given the frequency with which even purely domestic communications cross international borders, and given the growing amount of private data stored overseas, we are concerned that Executive Order 12333 permits the government to circumvent statutory or constitutional constraints on surveillance.

Sen. Dianne Feinstein, chair of the Senate Intelligence Committee, has acknowledged that Congress has been unable to “sufficiently” oversee surveillance conducted under Executive Order 12333.⁴ This underscores the need for a thorough assessment of that surveillance, and we are pleased by the PCLOB’s commitment to address this issue in the near term. We urge the PCLOB to assess fully:

- the extent to which the communications of U.S. persons and other non-target persons are collected and disseminated under the order;
- the constitutional and human rights concerns that the order raises;
- the use of the authority to collect bulk information domestically or overseas;
- the extent to which alternative statutory authorities can be used to achieve the same national security goals; and
- the need for enhanced privacy and oversight mechanisms.

2. Federal Government Use of Watchlists

Recently leaked documents confirm that the government’s bloated watchlist system is based on vague and overbroad criteria that give agencies near-unfettered discretion to blacklist people as “known or suspected terrorists.”⁵ The Terrorist Identities Datamart Environment (TIDE), the government's central repository of classified information that serves as the basis for various watchlists, including the master

³ In 2013, the ACLU and the Media Freedom and Information Access Clinic at Yale Law School filed a Freedom of Information Act lawsuit for information about the government’s use of Executive Order 12333. See Alex Abdo, *The Most Important Surveillance Order We Know Almost Nothing About*, ACLU BLOG OF RIGHTS (Dec. 30, 2013), <https://www.aclu.org/blog/national-security/most-important-surveillance-order-we-know-almost-nothing-about>.

⁴ See Ali Watkins, *Most of NSA’s Data Collection Authorized by Order Ronald Reagan Issued*, MCCLATCHY (Nov. 21, 2013), <http://www.mcclatchydc.com/2013/11/21/209167/most-of-nsas-data-collection-authorized.html>.

⁵ See Jeremy Scahill & Ryan Devereaux, *The Secret Government Rulebook For Labeling You A Terrorist*, THE INTERCEPT (July 23, 2014), <https://firstlook.org/theintercept/article/2014/07/23/blacklisted/>; Jeremy Scahill & Ryan Devereaux, *Barack Obama’s Secret Terrorist-Tracking System, by the Numbers*, THE INTERCEPT, (Aug. 5, 2014), <https://firstlook.org/theintercept/article/2014/08/05/watch-commander/>. ACLU, *US Government Watchlisting: Unfair Process and Devastating Consequences* (Mar. 2014), available at https://www.aclu.org/sites/default/files/assets/watchlist_briefing_paper_v3.pdf.

watchlist, or Terrorist Screening Database, contains more than 1 million names. The master watchlist, which is shared with federal agencies, state and local law enforcement, and at least 22 foreign governments, includes roughly 680,000 names.

The current watchlisting system ensnares innocent persons and targets racial and religious minorities disproportionately. The government uses a loose, poorly defined standard in determining who can be added to the master watchlist, and then pierces that standard with loopholes that permit watchlisting without even a showing of reasonable suspicion. The result is a watchlisting system that is unfair and discriminatory. For instance, Dearborn, Michigan—a city with fewer than 100,000 residents that is home to a large community of Arab Americans—has more watchlisted individuals than any city in the United States other than New York City.

In addition, inclusion on a watchlist raises significant privacy and civil liberties concerns. For example, when the government includes people in TIDE, it seeks out and collects their biometric data, including fingerprints, facial images, and DNA strands. When the government includes people on the master watchlist it can mean the inability to travel by air or sea, invasive screening at airports, denial of a U.S. visa or permission to enter the United States, or detention and questioning by U.S. or foreign authorities. These problems are compounded by the fact that the government fails to provide wrongly or mistakenly blacklisted individuals with an effective mechanism of redress. Such individuals are never told whether or why they are on a watchlist, let alone given a meaningful opportunity to contest their placement on a watchlist and clear their names. As a federal court recently recognized, the lack of a meaningful process for people to challenge their inclusion on the No Fly List, a subset of the master watchlist, violates the Fifth Amendment’s guarantee of due process.⁶

We urge the Board to examine whether:

- the government’s watchlist standards are appropriately narrow;
- the evidence being relied upon is accurate and credible;
- the manner in which the lists are used is consistent with the presumption of innocence and the right to a hearing; and
- the redress and periodic review procedures are consistent with basic constitutional requirements of fairness and due process.

3. Suspicious Activity Reporting (SAR) and eGuardian

Since at least 2008, the federal government has encouraged state and local law enforcement agencies to collect and report information that appears “suspicious” and that might have a nexus to terrorism. These “Suspicious Activity Reports,” or “SARs,” are then submitted to one of the nation’s 78 “fusion centers,” which are operated by state and local government agencies. If an analyst believes that a

⁶ *Latif et. al. v. Holder*, No. 3:10-CV-00750 (D. Or. June 24, 2014). The government has indicated its intent to revamp the No Fly List redress procedures, but we are concerned that, without external input, those procedures will not provide the minimum indicia of due process: notice, reasons, and a meaningful hearing before a neutral decision-maker.

report meets one or more SAR program standards, he or she will upload it to one or more national databases, such as the FBI's eGuardian system, where it can be accessed by the FBI and law enforcement agencies across the country.

We are concerned that the standards defining "suspicious activity" do not require any reasonable suspicion of criminal activity and easily encompass innocent or First Amendment-protected conduct. A Department of Justice regulation implemented in 1978 allows the collection, maintenance, and dissemination of "criminal intelligence information" about someone "only if there is reasonable suspicion that the individual is involved in criminal conduct or activity and the information is relevant to that criminal conduct or activity."⁷ The SAR programs subvert this regulation by deeming many innocuous activities as inherently suspicious and by encouraging state, local, and tribal law enforcement agencies, as well as private entities, to collect and disseminate information about such activities in the absence of reasonable suspicion. These programs encourage racial and religious profiling and chill First Amendment-protected conduct.

We commend the board for its commitment to examine the standards used by state and local authorities to report suspicious activities. As part of its review, we urge the Board to examine whether:

- the evidentiary standards for the SAR programs satisfy federal law and Constitutional precedent;
- the storage and dissemination of the data comply with federal law and Constitutional precedent; and
- the periodic review procedures are consistent with basic constitutional notions of fairness and due process.

4. Domestic FBI Operations

After 9/11, the U.S. government substantially downgraded legal restrictions on the Department of Justice and the FBI in particular, which were designed to remedy abuses and protect civil liberties during investigations. For example, the Attorney General's Guidelines on Domestic FBI Operations and an internal FBI guide to implementing them called the Domestic Investigations and Operations Guide (DIOG) were revised to permit the FBI to conduct pre-investigation "assessments" for unlimited periods and to use intrusive investigation techniques absent any suspicion of wrongdoing. These extraordinary authorities amplify many other problems, including racial profiling in national security and border integrity investigations.

Based on these authorities and other downgraded restrictions, the FBI has engaged in the following abusive behaviors:

- Through "domain management" assessments, the FBI collects, uses, and maps the demographic information of racial and ethnic communities. FBI documents obtained by the ACLU through the Freedom of Information Act show the agency has targeted minority communities for additional

⁷ 28 C.F.R. Part. 23 (1993).

intelligence gathering based primarily, if not entirely, on their religious, racial or ethnic makeup.

- The Attorney General's Guidelines and DIOG permit the FBI to deploy undercover agents or paid informants to infiltrate community religious and cultural institutions during pre-investigation "assessments," that is, in the absence of any suspicion of wrongdoing. These tactics generate distrust within the targeted communities and a fear among racial, religious and other minority communities that law enforcement views them with generalized suspicion and is monitoring their ordinary behavior.
- The FBI has also aggressively pressured American Muslim community and other community members to become informants for the FBI. It has particularly targeted immigrants who must rely on the government to process their immigration and citizenship applications in a fair and timely manner. While there is no recent and large-scale study of these incidents, there are reports of FBI intimidation, harassment and targeting of youth in particular.
- Informants and undercover FBI agents have used overly aggressive tactics in terrorism sting operations targeting individuals, including the mentally ill and poor, who are vulnerable to manipulation.⁸

In light of such examples, we urge to PCLOB to review how the Guidelines and DIOG impact law enforcement practices in minority and other communities in order to inform the Attorney General's assessment of whether revisions or additional safeguards are necessary.

5. Section 702 of FISA

On July 2, 2014, the PCLOB released its report examining surveillance activities conducted under Section 702 of FISA.⁹ Recent disclosures, however, have raised questions that were not fully addressed by the Board's report. For example, a Washington Post investigation of 160,000 communications collected under Section 702 found that 90% of account holders in the intercepted communications were not targets and that over half of the communications were to, from, or about US persons.¹⁰ In light of this information, it is now clear that the Board's report fell short of a full assessment of the privacy implications of Section 702 on U.S. persons and other non-targets, apparently due to false assertions by

⁸ See ACLU, *Unleashed and Unaccountable: The FBI's Unchecked Abuse of Authority* (Sep. 2013), available at <https://www.aclu.org/national-security/unleashed-and-unaccountable-fbis-unchecked-abuse-authority>; see also Human Rights Watch & Columbia Law School Human Rights Institute, *Illusion of Justice: Human Rights Abuses in US Terrorism Prosecutions* (July 2014), available at <http://www.hrw.org/reports/2014/07/21/illusion-justice-0>.

⁹ 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) available at <http://www.pclob.gov/All%20Documents/Report%20on%20the%20Section%20702%20Program/PCLOB-Section-702-Report.pdf> [hereinafter Report].

¹⁰ Barton Gellman, Julie Tate & Ashkan Soltani, *In NSA-intercepted Data, Those Not Targeted Far Outnumber the Foreigners Who Are: Files Provided By Snowden Show the Extent to Which Ordinary Web User are Caught in the Net*, (July 5, 2014), WASHINGTON POST, http://www.washingtonpost.com/world/national-security/in-nsa-intercepted-data-those-not-targeted-far-outnumber-the-foreigners-who-are/2014/07/05/8139adf8-045a-11e4-8572-4b1b969b6322_story.html?wpisrc=al_national.

the intelligence community that such information was unavailable. Indeed, the board repeatedly noted in its report that it was unable to assess the extent to which Section 702 led to the collection of U.S. or non-target information.¹¹ Moreover, recent disclosures raise concerns that information thought to be subject to existing Section 702 minimization procedures is still accessible by federal authorities, amplifying privacy concerns.¹²

Accordingly, we urge the Board to conduct further analysis of the use of Section 702, including:

- the extent to which US and non-target information is collected;
- the validity of assertions by the intelligence community that the number of U.S. and non-target communications cannot be estimated;
- the existence of alternative programs that would further the government's national security goals while simultaneously providing greater privacy protections;
- the scope and sufficiency of minimization procedures; and
- whether Section 702 complies with international law.

We would welcome the opportunity to meet with you about these potential areas of inquiry. If you have further questions, please feel free to contact Neema Singh Guliani (202-675-2322 or nguliani@aclu.org), Naureen Shah (202-675-2327 or nshah@aclu.org), or Arjun Sethi (202-715-0823 or asethi@aclu.org).

Sincerely,



Laura W. Murphy
Washington legislative Office
Director



Neema Singh Guliani
Legislative Counsel



Naureen Shah
Legislative Counsel

¹¹ See Report, *supra* note 11, at 10, 146-148.

¹² See Ryan Gallagher, *The Surveillance Engine: How the NSA Built Its Own Secret Google*, THE INTERCEPT (Aug. 25, 2014), <https://firstlook.org/theintercept/article/2014/08/25/icreach-nsa-cia-secret-google-crisscross-proton/>.



Arjun Sethi
Legislative Counsel