

August 1, 2013

Chairman David Medine
Rachel Brand
Elisebeth Collins Cook
James Dempsey
Patricia Wald
Privacy and Civil Liberties Oversight Board
Washington, D.C. 20427

Re: Workshop Regarding Surveillance Programs Operated Pursuant to Section 215 of the USA PATRIOT Act and Section 702 of Foreign Intelligence Surveillance Act (PCLOB-2013-0005)

Dear Privacy and Civil Liberties Oversight Board:

Our undersigned organizations provide the following comment in response to the public workshop conducted by the Privacy and Civil Liberties Oversight Board regarding surveillance programs operated pursuant to Section 215 of the PATRIOT Act and Section 702 of the Foreign Intelligence Surveillance Act (FISA).¹ We respectfully submit this comment to express our concern about the surveillance programs currently in place under Sections 215 and 702, and to urge PCLOB to recommend that the laws and associated procedures be conducted with sufficient consideration of government accountability, the people's right to know, privacy, and other fundamental civil liberties.

Introduction

As you know, PCLOB is charged with “advis[ing] the President and the departments, agencies, and elements of the executive branch to ensure that privacy and civil liberties are appropriately considered” in the development and implementation of all laws, regulations, and policies related to efforts to protect the United States from terrorism.² Critical to the current debate about domestic surveillance activities, PCLOB must review past and future surveillance programs not only for compliance with the law, but also to ensure that these programs sufficiently consider privacy and civil liberties concerns. In preparing advice on whether to retain or enhance a particular governmental power or policy, PCLOB must consider whether the government has established:

¹ 78 Fed. Reg. 39021 (June 28, 2013).

² Public Law 110–53, 121 Stat. 352.

- i. that the need for the power is balanced with the need to protect privacy and civil liberties;
- ii. that there is *adequate* supervision of the use by the executive branch of the power to ensure protection of privacy and civil liberties; and
- iii. that there are *adequate* guidelines and oversight to properly confine its use.³

In addition, PCLOB must oversee executive branch counterterrorism efforts to make certain that they “*appropriately* protect privacy and civil liberties” and “are consistent with governing laws, regulations, and policies regarding privacy and civil liberties.”⁴

In sum, the role of PCLOB is to ensure that our best efforts to keep this country safe are balanced with an “adequate” and “appropriate” respect for the privacy and civil liberties of every person in the United States. We urge PCLOB to take this opportunity to thoroughly review our national security laws and policies for compliance with this standard. Recent revelations of NSA surveillance programs raise serious concerns about the interpretation and application of laws that have provided the executive branch with overly broad authority to collect personal, sensitive information. Changes in the law, and in the policies and procedures that implement the law, are needed to restore equilibrium between surveillance authorities and constitutional rights.

Sections 215 and 702 Raise Serious Concerns

The recent disclosures have revealed troubling, aggressive interpretations and applications of Section 215 of the PATRIOT Act and Section 702 of the Foreign Intelligence Surveillance Act (FISA). Section 215 has been used to collect telephony metadata from all customers of major telecommunications companies, an interpretation that seemingly distorts the statutory requirement of “relevance” to an antiterrorism investigation. Section 702 has been used to create bulk surveillance programs that collect the communications of U.S. persons (citizens and permanent legal residents) and people located within the United States simply because they are in contact with non-U.S. persons.

The revelations have underscored the dangers of secret law, wherein the laws passed by Congress are interpreted and applied behind closed doors by a small group of government officials and federal judges. Laws made and implemented in secret restrict the opportunity for oversight, public debate, and legislative correction—ultimately threatening the foundations of our constitutional democracy. When the American people are not given the opportunity to influence government policies, even those associated with national security concerns, then democracy fails.

³ *Id.* at 353 (emphasis added).

⁴ *Id.*

Also of concern is that the authorizations for programmatic surveillance of millions of Americans are issued following *ex parte* proceedings, during which only the government has the opportunity to present arguments. Although we are not calling into question the competence of the judges on the Foreign Intelligence Surveillance Court (FISC), no judge should be expected to properly adjudicate a case without an adversarial proceeding. In addition, due to the structure of Sections 215 and 702, the only parties that can challenge a ruling by FISC are the government and the entity approached to hand over the records and communications—the persons whose records are being collected by the government have no awareness of the proceeding, much less an opportunity to speak on their own behalf.

Although other courts do use *ex parte* proceedings to issue search warrants, these warrants are justified by probable cause and describe with particularity the places to be searched and the items to be seized. In addition, *ex parte* search warrants can be challenged later in court. By contrast, the rise of programmatic surveillance now sees the government request authorization for bulk data collection, wherein the government collects data related to millions of U.S. persons without particularized targeting or individualized suspicion. Because FISC grants approval in secret and prohibits communications providers from disclosing the existence of orders, an American citizen whose information is collected by the government has no recourse to challenge the order. Without an advocate representing the American public, their interests are diminished.

We believe it is important that the government acts to prevent our country from suffering devastating and violent attacks. However, the nature of democracy and our Constitution also demands that the government remain accountable to the public and transparent to its citizenry. Below, we present a list of recommendations that will help preserve fundamental rights while doing nothing to diminish the ability of the government to keep our nation safe.

Recommendations

We urge you to advise the President to take action to ensure critical reforms that:

- **Ensure that all government surveillance programs that affect privacy and civil liberties have a unique benefit.** Convenience is not a substitute for constitutional rights. To justify the continuance of surveillance programs that affect civil liberties and privacy, the executive branch must provide detailed analysis of the effectiveness of each program. The executive branch should draft and submit a classified report each year to Congress and PCLOB, and release a declassified version to the public. The report must include a particular emphasis on each program’s unique benefit and provide evidence that justifies the continuation of the surveillance programs in question.
 - “Unique benefit” in this context means detailed, convincing evidence that information necessary to impede violent attacks could not be gained by less

invasive surveillance measures. The report should contain the number of instances in which surveillance data both *did* and *did not* provide a unique benefit to thwarting a threat to national security. The report should further detail, to the extent possible while respecting national security interests, each instance and the unique role (or lack thereof) played by surveillance data.

- Considering the June 2013 disclosures of bulk domestic surveillance, the executive branch should provide a detailed, specific report on the recently revealed programs that lays out the unique benefits provided by each. The report should date back to October 2001, when the PATRIOT Act was first passed.
- **Ensure that the rights and interests of the American public are protected during FISC hearings.** We urge the creation of a panel of *ad litem* attorneys to represent the American public whenever the government applies for surveillance orders before FISC. The *ad litem* attorneys would be housed in PCLOB and report directly to the Executive Director, thereby establishing a measure of independence and separation from the executive branch, and would have security clearance sufficient to review all evidence in government surveillance requests. The attorneys would also have the opportunity to appeal adverse decisions to the Foreign Intelligence Surveillance Court of Review. We strongly encourage the adoption of a rule stating that non-government attorneys must comprise no less than 30 percent of this attorney panel, that their terms be limited to no more than five years, and that attorneys be randomly selected from the panel to appear before the Court in each pertinent case.
- **Facilitate congressional and public debate around critical national security issues by aligning the sunsets for Sections 215 and 702.** Currently, Section 215 (and Section 206) of the PATRIOT Act will sunset on June 1, 2015, but Section 702 of FISA will not sunset until December 31, 2017. Aligning the sunsets to June 1, 2015, would allow Congress and the nation to appropriately debate the full scope of our national security and surveillance programs. In this vein, we support the “FISA Accountability and Privacy Protection Act of 2013,”⁵ introduced in the Senate last month by Senator Patrick Leahy (D-VT) and cosponsored by a bipartisan group of nine other Senators. Among other things, this bill would align the sunsets associated with FISA and the PATRIOT Act to June 1, 2015.
- **Ensure accountability by clearly delineating the retention period for all collected metadata and information; and delimiting with whom such information can be shared, under what circumstances, and with what reporting requirements.** The

⁵ U.S. Senate, “FISA Accountability and Privacy Protection Act of 2013” (S. 1215), Introduced June 24, 2013, by Senator Patrick Leahy. <http://www.gpo.gov/fdsys/pkg/BILLS-113s1215is/pdf/BILLS-113s1215is.pdf> (Downloaded July 29, 2013)

executive branch should set specific limits on the retention of collected metadata and information and clear processes for its disposition. As with all information in the government's possession with privacy impact implications, the information should have clearly stated rules on its sharing and on how any permitted sharing will be documented and recorded.

- **Facilitate transparency by publicly releasing declassified versions of legal documents that substantively interpret the PATRIOT Act and FISA.** These documents include copies or summaries of FISC opinions, Office of Legal Counsel (OLC) memos, and other documents necessary for public understanding of the scope of surveillance authorities, safeguards for privacy rights and civil liberties, and the historical development of the law since 2001. We support the "Ending Secret Law Act,"⁶ introduced by Senator Jeff Merkley (D-OR) and cosponsored by a bipartisan coalition of 14 other Senators, which would require the Department of Justice to unseal or release summaries of FISC opinions.

We appreciate that releasing declassified documents will not be an easy task. Indeed, we have heard a number of arguments against the public release of FISC opinions in particular; these arguments, however, are insufficient.⁷ The public interest in remaining cognizant of our government's actions outweighs the difficulties in preparing and releasing declassified FISC opinions and other legal documents. The release of these documents would dispel the atmosphere of speculation and confusion that now surrounds the government's activities. It would further promote public dialogue and an informed citizenry by clearly declaring the legal principles underlying electronic surveillance and other national security measures.

The executive branch should also issue a mandate that all such legal documents deemed to not be suitable for declassification at this time will be automatically reviewed for declassification and release every five years.

- **Promote government accountability and greater public awareness by requiring the executive branch to produce and release reports on national security policies and surveillance programs.** The executive branch should draft and submit detailed, classified reports to PCLOB and Congress, and release unclassified versions to the public. These reports should be issued on a regular basis as determined by Congress. The reports should contain at least:

⁶ U.S. Senate, "Ending Secret law Act" (S. 1130), Introduced June 11, 2013, by Senator Jeff Merkley. <http://www.gpo.gov/fdsys/pkg/BILLS-113s1130is/pdf/BILLS-113s1130is.pdf> (Downloaded July 29, 2013)

⁷ Aimee Thomson and Angela Canterbury, "Secret Court Resists Releasing Surveillance Opinions," *POGO Blog*, July 12, 2013. <http://www.pogo.org/blog/2013/07/20130712-secret-court-resists-releasing-surveillance-opinions.html>

- The number of orders issued by FISC, distinguished by program, time period, and recipients of orders.
 - The number of Section 702-authorized directives issued by the Attorney General (AG) and the Director of National Intelligence (DNI) to electronic communication service providers requesting information, distinguished by time period and the entity that received the order. Because FISC only authorizes the *creation* of a Section 702 surveillance program, statistics regarding the directives issued by the AG and the DNI to service providers is needed to fully appreciate the scope of these programs.
 - Statistics and analysis regarding the collection, use, and storage of communications under all surveillance programs, including Section 215 and Section 702 programs. The statistics should distinguish between and cover both transactional data (“metadata”) and content data, as well as distinguish between and cover both U.S. persons and non-U.S. persons.
 - Detailed minimization procedures for any and all agencies which can be reasonably expected to receive unminimized information collected under all surveillance programs, including Section 215 and Section 702 programs. These procedures should address the treatment of privacy-protected information as well as the treatment of information traditionally protected by a statutory or common law privilege, such as the attorney-client privilege.
 - Detailed analysis of the effectiveness of each program’s targeting and minimization procedures. The analysis would include the number of U.S. persons’ communications inadvertently collected as compared to the number of all persons’ communications collected.
 - Detailed analysis of the effectiveness of internal mechanisms that protect against unauthorized access to databases of collected data.
 - Detailed analysis exploring how frequently information collected under all surveillance programs has been used for domestic law enforcement purposes, as compared to use for national security or foreign intelligence purposes. In particular, the analysis should identify how many times information collected under Section 702 is flagged because it contains evidence of a crime not within the scope of foreign intelligence or national security.
 - As with the legal documents discussed above, the executive branch should mandate that all reports described herein deemed to not be suitable for declassification at this time will be automatically reviewed for declassification and release every five years.
- **Encourage transparency by limiting the gag-orders on all entities that receive Section 215 or 702 orders.** Congress should change FISA and the PATRIOT Act to limit to 30 days the period during which the recipient of FISC order can be required not to

disclose existence of the order. The government would then have the opportunity to prove to a judge that there is reason to believe that a specified and articulable harm would result unless the “gag order” is extended.

PCLOB bears the critical responsibility of protecting the individual rights of the American people. We hope that PCLOB will seriously review this comment and other recommendations from the transparency and civil liberties communities ahead of its report on how to improve Sections 215 and 702.

Sincerely,

Angela Canterbury
Director of Public Policy
Project On Government Oversight (POGO)

Kel McClanahan
Executive Director
National Security Counselors

Patrice McDermott
Executive Director
OpenTheGovernment.org

Founded in 1981, **Project On Government Oversight (POGO)** is a nonpartisan independent watchdog that champions good government reforms. POGO’s investigations into corruption, misconduct, and conflicts of interest achieve a more effective, accountable, open, and ethical federal government. As such, POGO has a keen interest in how government policies affect civil liberties and national security. We believe that as we seek to keep the nation safe, we must ensure other interests such as privacy, constitutional rights, government accountability, and the people’s right to know are duly respected.

National Security Counselors was founded to further the twin ideals that the public needs to be as informed as possible about what its government does in the name of national security, and that people entangled in legal matters in this field should have reasonable access to knowledgeable legal assistance, regardless of income. To that end, NSC exists to perform four primary functions: to lawfully acquire from the government material related to national security matters and distribute it to the public, to use this material in the creation of original publications discussing the respective subjects, to advocate for intelligent reform in the national security and

information and privacy arenas, and to provide a low-cost alternative to certain deserving clients involved in security law or information and privacy law-related proceedings.

OpenTheGovernment.org believes that the People have a right to information held by and for our government, that transparency is essential to ensuring integrity and accountability in the operation of our governing institutions, and that openness helps to ensure that policies affecting our health, safety, security and freedoms place the public good and well-being above the influence of special interests. Making government as open as possible also fosters confidence in representative government and encourages public participation in civic affairs, an essential feature of our form of government. For all these reasons, OpenTheGovernment.org seeks to advance the public's right to know and to reduce unnecessary secrecy in government.