PRIVACY & CIVIL LIBERTIES OVERSIGHT BOARD

STATEMENT

OF

DAVID MEDINE, CHAIRMAN

PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD

BEFORE THE

HOUSE JUDICIARY COMMITTEE

HEARING ENTITLED

"RECOMMENDATIONS TO REFORM FOREIGN INTELLIGENCE PROGRAMS"

FEBRUARY 4, 2014

STATEMENT OF DAVID MEDINE
CHAIRMAN, PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD
BEFORE THE HOUSE JUDICIARY COMMITTEE
HEARING ENTITLED
"RECOMMENDATIONS TO REFORM FOREIGN INTELLIGENCE PROGRAMS"
FEBRUARY 4, 2014

I. Introduction

Thank you for the opportunity to appear today before the House Judiciary Committee as you evaluate potential reforms to government surveillance programs.

I am the chairman of the Privacy and Civil Liberties Oversight Board ("PCLOB"), an independent executive branch agency tasked with ensuring that our nation's counterterrorism efforts are balanced with the need to protect civil liberties and privacy. On January 23, 2014, the Board released a comprehensive public report addressing the bulk telephone records program conducted by the National Security Agency ("NSA") under Section 215 of the USA PATRIOT Act, as well as the operations of the Foreign Intelligence Surveillance Court.[1] The report, which is available at www.pclob.gov, contains an in-depth examination of the Section 215 program, including its operation, history, legality, constitutionality, and an analysis of whether it appropriately balances national security with privacy and civil liberties. The report also addresses the operations of the Foreign Intelligence Surveillance Court and the issue of transparency in government surveillance programs. The Board has made twelve specific recommendations for reform in these areas, ten of which were unanimous among the Board's five members.[2]

The Board looks forward to working with Congress and the executive branch in the coming months as reforms to the government's surveillance practices are being considered.[3]

---

1 *See* Privacy and Civil Liberties Oversight Board, Report on the Telephone Records Program Conducted under Section 215 of the USA PATRIOT Act and on the Operations of the Foreign Intelligence Surveillance Court (Jan. 23, 2014), *available at* http://www.pclob.gov/.

2 The Board's next public report will examine the surveillance program being conducted by the National Security Agency under Section 702 of the FISA Amendments Act of 2008, addressing whether, in the Board's view, the program is consistent with statutory authority, complies with the Constitution, and strikes the appropriate balance between national security and privacy and civil liberties.

3 While these prepared remarks describe the views of the full Board, as reflected in its January 23, 2014 report (including the separate minority statements included with that report), my spoken comments at the hearing represent my own personal views.

II. The PCLOB

The PCLOB is an independent bipartisan agency within the executive branch. The Board's creation was a recommendation of the 9/11 Commission, which advised in its final report that "there should be a board within the executive branch to oversee adherence to the guidelines we recommend and the commitment the government makes to defend our civil liberties."[4]

The Board was established in its present form as an independent agency by the Implementing Recommendations of the 9/11 Commission Act of 2007,[5] but it did not become fully operational with all five Board members until May of last year.[6] It is comprised of four part-time members and a full-time chairman, each serving staggered six-year terms, all appointed by the President and confirmed by the Senate.[7] The Board's authorizing statute gives it two primary responsibilities: (1) to "analyze and review actions the executive branch takes to protect the Nation from terrorism, ensuring that the need for such actions is balanced with the need to protect privacy and civil liberties," and (2) to "ensure that liberty concerns are appropriately considered in the development and implementation of laws, regulations, and policies related to efforts to protect the Nation against terrorism."[8]

---

4 THE 9/11 COMMISSION REPORT: FINAL REPORT OF THE NATIONAL COMMISSION ON TERRORIST ATTACKS UPON THE UNITED STATES, at 395 (2004). The National Commission on Terrorist Attacks on the United States (known as the 9/11 Commission) was a bipartisan panel established to "make a full and complete accounting of the circumstances surrounding" the September 11, 2001, terrorist attacks, and to provide "recommendations for corrective measures that can be taken to prevent acts of terrorism." Intelligence Authorization Act for Fiscal Year 2003, Pub. L. No. 107-306, § 602(4), (5), 116 Stat. 2383, 2408 (2002).

5 Pub. L. No. 110-53, § 801(a), 121 Stat. 266, 352-58 (2007).

6 In August 2012, the Board's four part-time members were confirmed by the Senate, providing the reconstituted Board with its first confirmed members and a quorum to begin operations. I was confirmed as chairman of the Board (its only full-time member) on May 7, 2013, and sworn in on May 29, five days before news stories based upon the NSA leaks began to appear.

7 The five members of the Board, and their respective terms, are as follows:

- Rachel L. Brand, whose term ends January 29, 2017.
- Elisebeth Collins Cook, whose first term ended January 29, 2014. On January 6, 2014, Ms. Cook was nominated for a second term ending January 29, 2020. Under the Board's authorizing statute, as a result of this nomination, Ms. Cook can continue to serve through the end of the Senate's current session and, if confirmed before then, through January 29, 2020.
- James X. Dempsey, whose term ends January 29, 2016.
- David Medine (chairman), whose term ends January 29, 2018.
- Patricia M. Wald, whose term ends January 29, 2019.

8 42 U.S.C. § 2000ee(c).

III. The Board's Report on the Section 215 Telephone Records Program and the FISA Court

Last June, shortly after the first news articles appeared disclosing the existence of a previously unknown NSA program conducted under Section 215, as well as details regarding surveillance conducted under Section 702 of the FISA Amendments Act, a bipartisan group of thirteen U.S. Senators asked the PCLOB to investigate those programs and to produce an unclassified report, "so that the public and the Congress can have a long overdue debate" about the privacy issues they raised.[9] A subsequent letter from House Minority Leader Nancy Pelosi requested that the Board also consider the operations of the Foreign Intelligence Surveillance Court ("FISC" or "FISA court"), which approved the two programs. On June 21, 2013, the Board met with President Obama and his senior staff at the White House, and the President asked the Board to review "where our counterterrorism efforts and our values come into tension."[10]

In response to these congressional and presidential requests, the Board initiated a study of the Section 215 and 702 programs and the operation of the FISA court.[11] This study included classified briefings with officials from the Office of the Director for National Intelligence ("ODNI"), NSA, Department of Justice, Federal Bureau of Investigation ("FBI"), and Central Intelligence Agency ("CIA"). Board members also met with White House staff, a former presiding judge of the FISA court, academics, privacy and civil liberties advocates, technology and communications companies, and trade associations. In addition, the Board received a demonstration of the Section 215 program's operation and capabilities at the NSA. The Board has been provided access to classified opinions by the FISA court, various inspector general reports, and additional classified documents relating to the operation and effectiveness of the programs. At every step of the way, the Board has received the full cooperation of the intelligence agencies.

As part of its study, and consistent with our statutory mandate to operate publicly where possible, the Board held two public forums. The first was a day-long public workshop held in Washington, D.C., on July 9, 2013, comprised of three panels addressing different aspects of the Section 215 and 702 programs. The panelists provided input on the legal, constitutional, technology, and policy issues implicated by the two programs. The

---

9 Letter from Senator Tom Udall *et al*. to the Privacy and Civil Liberties Oversight Board (June 12, 2013), *available at* http://www.pclob.gov/.

10 *See* Letter from Democratic Leader Nancy Pelosi to Chairman David Medine (July 11, 2013), *available at* http://www.pclob.gov/; Remarks by the President in a Press Conference at the White House (Aug. 9, 2013), *available at* http://www.whitehouse.gov/the-press-office/2013/08/09/remarks-president-press-conference.

11 Prior to my confirmation as chairman, the four part-time Board members already had identified implementation of the FISA Amendments Act as a priority for oversight. As a result, the Section 702 program already was familiar to the majority of the Board by June 2013.

first panel addressed the legality of the programs, and included comments from a former FISA court judge regarding the operation of that court. Because technological issues are central to the operations of both programs, the second panel was comprised of technology experts. The third panel included academics and members of the advocacy community; panelists were invited to provide views on the policy implications of the NSA programs and what changes, if any, would be appropriate.

As the Board's study of the NSA surveillance programs moved forward, the Board began to consider possible recommendations for program changes. At the same time, the Board wanted to try to identify any unanticipated consequences of reforms it was considering. Accordingly, on November 4, 2013, the Board held a public hearing in Washington, D.C. The hearing began with a panel of current government officials who addressed the value of the programs and the potential impact of proposed changes. The second panel, designed to explore the operation of the FISA court, consisted of another former FISC judge, along with a former government official and a private attorney who both had appeared before the FISC. Finally, the Board heard from a diverse panel of experts on potential Section 215 and 702 reforms.[12]

Based on the information and input made available to the Board, we conducted a detailed analysis of applicable statutory authorities, the First and Fourth Amendments to the Constitution, and privacy and civil liberties policy issues raised by the Section 215 program. The Board provided its draft description of the operation of the FISA court (but not our recommendations) to the court's staff to ensure that this description accurately portrayed the court's processes. The Board also provided draft portions of its analysis regarding the effectiveness of the Section 215 program (but not our conclusions and recommendations) to the U.S. Intelligence Community to ensure that our factual statements were correct and complete. While the Board's report was subject to classification review, none of the changes resulting from that process affected our analysis or recommendations. There was no outside review of the substance of our analysis or recommendations.

During the time that the PCLOB was conducting its study, members of Congress introduced a variety of legislative proposals to address the Section 215 and 702 programs, and the executive branch simultaneously was engaging in several internal reviews of the programs. To ensure that the PCLOB's recommendations would be considered as part of this ongoing debate, the Board divided its study into two separate reports. The first report, issued on January 23, 2014, covers the PCLOB's analysis and recommendations concerning operation of the Section 215 program and the FISA court. The second report, which also

[12] Transcripts of the Board's July 2013 public workshop and its November 2013 public hearing are available at http://www.pclob.gov/.

will be public and unclassified,[13] will contain the PCLOB's analysis and recommendations concerning the Section 702 program.

Proposals for modifications to the Section 215 program and the operation of the FISA court also were under active consideration by the White House while we were conducting our study. Pursuant to the Board's statutory duty to advise the President and elements of the executive branch to ensure that privacy and civil liberties are appropriately considered in the development and implementation of legislation and policies, and to provide advice on proposals to retain or enhance a particular counterterrorism power, the PCLOB briefed senior White House staff on the Board's tentative conclusions on December 5, 2013. We provided a near-final draft of the Board's conclusions and recommendations on Section 215 and the operations of the FISA court to the White House on January 3, 2014. On January 8, the full Board met with the President, the Vice President, and senior officials to present the Board's conclusions and the views of individual Board members.

Our first report consists of seven sections, five of which address the Section 215 telephone records program. The report begins by describing in detail how the program works. To put the present-day operation of the program in context, the report also recounts its history, including its evolution from predecessor intelligence activities. Turning to the Board's analysis, the report then addresses whether the telephone records program is consistent with applicable statutory requirements. It then addresses the constitutional issues raised by the program under both the First and Fourth Amendments. Finally, the report examines the potential benefits of the Section 215 program, its efficacy in achieving its purposes, and the impact of the program on privacy and civil liberties, before presenting the Board's conclusion that reforms are needed.

In addition to examining the Section 215 program, the Board's report also addresses the operations of the FISA court, proposing a new approach that, in appropriate cases, would allow the judges serving on that court to hear from a Special Advocate. The final section of the report addresses the issue of transparency as it relates to government surveillance activities. The report also includes separate statements by Board members Rachel Brand and Elisebeth Collins Cook. Although these two members joined in ten of the twelve recommendations made in the report, as outlined below, they wrote separately to explain their disagreement with the remaining two recommendations and with some of the Board's analysis.

While the Board's report includes a number of detailed conclusions and recommendations, it does not purport to answer all questions. The Board welcomes the

[13] It is possible that the report on the Section 702 program will also include a classified annex.

opportunity for further dialogue within the executive branch and with Congress about the issues raised in its report and how best to implement the Board's recommendations.

IV. The Board's Findings and Analysis

A. Background: Description and History of the Section 215 Program

The NSA's telephone records program is operated under an order issued by the FISA court pursuant to Section 215 of the Patriot Act, an order that is renewed approximately every ninety days. The program is intended to enable the government to identify communications among known and unknown terrorism suspects, particularly those located inside the United States. When the NSA identifies communications that may be associated with terrorism, it issues intelligence reports to other federal agencies, such as the FBI, that work to prevent terrorist attacks. The FISC order authorizes the NSA to collect nearly all call detail records generated by certain telephone companies in the United States, and specifies detailed rules for the use and retention of these records. Call detail records typically include much of the information that appears on a customer's telephone bill: the date and time of a call, its duration, and the participating telephone numbers. Such information is commonly referred to as a type of "metadata." The records collected by the NSA under this program do not, however, include the content of any telephone conversation.

After collecting these telephone records, the NSA stores them in a centralized database. Initially, NSA analysts are permitted to access the Section 215 calling records only through "queries" of the database. A query is a search for a specific number or other selection term within the database. Before any specific number is used as the search target or "seed" for a query, one of twenty-two designated NSA officials must first determine that there is a reasonable, articulable suspicion ("RAS") that the number is associated with terrorism. Once the seed has been RAS-approved, NSA analysts may run queries that will return the calling records for that seed, and conduct "contact chaining" to develop a fuller picture of the seed's contacts. Contact chaining enables analysts to retrieve not only the numbers directly in contact with the seed number (the "first hop"), but also numbers in contact with all first hop numbers (the "second hop"), as well as all numbers in contact with all second hop numbers (the "third hop").

In 2012, the FISA court approved a new and automated method of performing queries, one that is associated with a new infrastructure implemented by the NSA to

process its calling records.[14] The essence of this new process is that, instead of waiting for individual analysts to perform manual queries of particular selection terms that have been RAS approved, the NSA's database periodically performs queries on all RAS-approved seed terms, up to three hops away from the approved seeds. The database places the results of these queries together in a repository called the "corporate store." The ultimate result of the automated query process is a repository, the corporate store, containing the records of all telephone calls that are within three "hops" of every currently approved selection term.[15]

The Section 215 telephone records program has its roots in counterterrorism efforts that originated in the immediate aftermath of the September 11 attacks. The NSA began collecting telephone metadata in bulk as one part of what became known as the President's Surveillance Program. From late 2001 through early 2006, the NSA collected bulk telephony metadata based upon presidential authorizations issued every thirty to forty-five days. In May 2006, the FISC first granted an application by the government to conduct the telephone records program under Section 215.[16] The government's application relied heavily on the reasoning of a 2004 FISA court opinion and order approving the bulk collection of Internet metadata under a different provision of FISA.[17]

On June 5, 2013, the British newspaper *The Guardian* published an article based on unauthorized disclosures of classified documents by Edward Snowden, a contractor for the NSA, which revealed the telephone records program to the public. On August 29, 2013, FISC Judge Claire Eagan issued an opinion explaining the court's rationale for approving the Section 215 telephone records program.[18] Although prior authorizations of the program had been accompanied by detailed orders outlining applicable rules and minimization procedures, this was the first judicial opinion explaining the FISA court's legal reasoning in authorizing the bulk records collection. The Section 215 program was reauthorized most recently by the FISC on January 3, 2014.

Over the years, a series of compliance issues were brought to the attention of the FISA court by the government. However, none of these compliance issues involved significant intentional misuse of the system. Nor has the Board seen any evidence of bad faith or misconduct on the part of any government officials or agents involved with the

---

14 This "automated query process" was first approved for use by the FISA court in late 2012. Primary Order at 11 n.11.

15 *See* Primary Order at 11.

16 *See* Order, *In re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things*, No. BR 06-05 (FISA Ct. May 24, 2006).

17 *See* Opinion and Order, No. PR/TT [*redacted*] (FISA Ct.).

18 *See* Amended Memorandum Opinion, *In re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things*, No. BR 13-109 (FISA Ct. Aug. 29, 2013).

program.[19] Rather, the compliance issues were recognized by the FISC — and are recognized by the Board — as a product of the program's technological complexity and vast scope, illustrating the risks inherent in such a program.

B. Statutory and Constitutional Considerations Regarding the Section 215 Program

The Board has concluded that Section 215 of the Patriot Act does not provide an adequate legal basis to support the NSA's bulk telephone records program. Section 215 is designed to enable the FBI to acquire records that a business has in its possession, as part of an FBI investigation, when those records are relevant to the investigation. Yet the operation of the NSA's bulk telephone records program bears almost no resemblance to that description. While the Board believes that this program has been conducted in good faith to vigorously pursue the government's counterterrorism mission and appreciates the government's efforts to bring the program under the oversight of the FISA court, it concludes that the program is not authorized by Section 215.

There are four grounds upon which we have concluded that the NSA's program fails to comply with Section 215. First, the telephone records acquired under the program have no connection to any specific FBI investigation at the time of their collection. Second, because the records are collected in bulk — potentially encompassing all telephone calling records across the nation — they cannot be regarded as "relevant" to any FBI investigation as required by the statute without redefining that word in a manner that is circular, unlimited in scope, and out of step with the case law from analogous legal contexts involving the production of records. Third, the program operates by putting telephone companies under an obligation to furnish new calling records on a daily basis as they are generated (instead of turning over records already in their possession) — an approach lacking foundation in the statute and one that is inconsistent with FISA as a whole. Fourth, the statute permits only the FBI to obtain items for use in its investigations; it does not authorize the NSA to collect anything.

In addition, we conclude that the program violates the Electronic Communications Privacy Act. That statute prohibits telephone companies from sharing customer records with the government except in response to specific enumerated circumstances, which do not include Section 215 orders.

---

[19] Neither has the Board seen any evidence that would suggest any telephone providers did not rely in good faith on orders of the FISC when producing metadata to the government.

Finally, we do not agree that the NSA's program can be considered statutorily authorized because Congress twice delayed the expiration date of Section 215 during the operation of the program without amending the statute. The "reenactment doctrine," under which Congress is presumed to have adopted settled administrative or judicial interpretations of a statute, does not trump the plain meaning of a law, and cannot save an administrative or judicial interpretation that contradicts the statute itself. Moreover, the circumstances presented here differ in pivotal ways from any in which the reenactment doctrine has ever been applied, and applying the doctrine here would undermine the public's ability to know what the law is and hold their elected representatives accountable for their legislative choices.

The Board also believes that the NSA's bulk telephone records program raises concerns under both the First and Fourth Amendments to the United States Constitution. Our report explores those concerns, explaining that while government officials are entitled to rely on existing Supreme Court doctrine in formulating policy, the existing doctrine does not fully answer whether the Section 215 program is constitutionally sound. In particular, the scope and duration of the program are beyond anything ever before confronted by the courts, and as a result of technological developments, the government possesses capabilities to collect, store, and analyze data not available when existing Supreme Court doctrine was developed. Without seeking to predict the direction of changes in that doctrine, the Board urges as a policy matter that the government consider how to preserve underlying constitutional guarantees in the face of modern communications technology and surveillance capabilities.

C. Policy Considerations Regarding the Section 215 Program

The Section 215 telephone records program was intended to function as a unique tool to help combat the very real threat of terrorism faced today by the United States — a tool that, it was hoped, would help investigators piece together the networks of terrorist groups and the patterns of their communications with a speed and comprehensiveness not otherwise available. However, the Board has concluded that the program has shown only minimal value in safeguarding the nation from terrorism. Based on the information provided to the Board, including classified briefings and documentation, we have not identified a single instance involving a threat to the United States in which the program made a concrete difference in the outcome of a counterterrorism investigation. Moreover, the Board is aware of no instance in which the program directly contributed to the discovery of a previously unknown terrorist plot or the disruption of a terrorist attack. And we believe that in only one instance over the past seven years has the program arguably contributed to the identification of an unknown terrorism suspect (a suspect who was not involved in planning a terrorist attack, and who might have been discovered by the FBI without the contribution of the NSA's program).

The Board's review suggests that where the telephone records collected by the NSA under its Section 215 program have provided value, they have done so primarily in two ways: by offering additional leads regarding the contacts of terrorism suspects already known to investigators, and by demonstrating that foreign terrorist plots do *not* have a U.S. nexus. While the former can help investigators confirm suspicions about the target of an inquiry or about persons in contact with that target, our review suggests that the Section 215 program offers little unique value but largely duplicates the FBI's own information-gathering efforts. And while eliminating a U.S. nexus to foreign plots can help the intelligence community focus its limited investigatory resources in time-sensitive situations by channeling efforts where they are needed most, our report questions whether the American public should accept the government's routine collection of all of its telephone records because it helps in cases where there is no threat to the United States.

The Board also has analyzed the implications of the Section 215 program for privacy and civil liberties and has concluded that these implications are serious. Because telephone calling records can reveal intimate details about a person's life, particularly when aggregated with other information and subjected to sophisticated computer analysis, the government's collection of a person's entire telephone calling history has a significant and detrimental effect on individual privacy. The circumstances of a particular call can be highly suggestive of its content, such that the mere record of a call potentially offers a window into the caller's private affairs. Moreover, when the government collects *all* of a person's telephone records, storing them for five years in a government database that is subject to high-speed digital searching and analysis, the privacy implications go far beyond what can be revealed by the metadata of a single telephone call.

Beyond such individual privacy intrusions, permitting the government to routinely collect the calling records of the entire nation fundamentally shifts the balance of power between the state and its citizens. With its powers of compulsion and criminal prosecution, the government poses unique threats to privacy when it collects data on its own citizens. Government collection of personal information on such a massive scale also courts the ever-present danger of "mission creep." An even more compelling danger is that personal information collected by the government will be misused to harass, blackmail, or intimidate, or to single out for scrutiny particular individuals or groups. While the danger of such abuse may seem remote today — we have seen no indication that anything of this sort is occurring at the NSA[20] — the risk is more than merely theoretical, given the history of the government's abuse of personal information during the twentieth century.

---

[20] The Board's report emphasizes that we have seen no evidence suggesting that the NSA is misusing the telephone records it acquires under this program for any purpose other than legitimate efforts to combat terrorism. The agency's incidents of non-compliance with the rules approved by the FISA court have generally involved unintentional mistakes resulting from the scope and complexity of the program.

Furthermore, the government's bulk collection of telephone records can be expected to have a chilling effect on the free exercise of speech and association, because individuals and groups engaged in sensitive or controversial work have less reason to trust in the confidentiality of their relationships as revealed by their calling patterns. Inability to expect privacy vis-à-vis the government in one's telephone communications means that people engaged in wholly lawful activities — but who for various reasons justifiably do not wish the government to know about their communications — must either forgo such activities, reduce their frequency, or take costly measures to hide them from government surveillance. The telephone records program thus hinders the ability of advocacy organizations to communicate confidentially with members, donors, legislators, whistleblowers, members of the public, and others. For similar reasons, awareness that a record of all telephone calls is stored in a government database may have debilitating consequences for communication between journalists and sources.

Detailed rules limit the NSA's *use* of the telephone records it collects, and the Board's report describes them at length. But while those rules offer many valuable safeguards designed to curb the intrusiveness of the program, in the Board's view they cannot fully ameliorate the implications for privacy, speech, and association that follow from the government's ongoing *collection* of virtually all telephone records of every American.

Any governmental program that entails such costs to privacy and civil liberties requires a strong showing of efficacy. As the 9/11 Commission recommended: "The burden of proof for retaining a particular governmental power should be on the executive, to explain," among other things, "that the power actually materially enhances security."[21] The Board has concluded that the NSA telephone records program conducted under Section 215 does not meet that standard, and that its modest contribution to counterterrorism efforts is outweighed by its implications for privacy, speech, and association.

D. Issues Concerning Operation of the Foreign Intelligence Surveillance Court and Transparency of Surveillance Programs

The Board's report also addresses the operation of the FISA court. The FISA court was created by the Foreign Intelligence Surveillance Act of 1978 ("FISA"), to provide a procedure under which the Attorney General could obtain a judicial warrant authorizing the use of electronic surveillance in the United States for foreign intelligence purposes. Over time, the scope of FISA and the jurisdiction of the FISA court have evolved. Initially, the FISC's sole role was to approve individualized FISA warrants for electronic surveillance relating to a specific person, a specific place, or a specific communications account or

[21] 9/11 Commission Report, *supra*, at 394-95.

device. Beginning in 2004, the role of the FISC changed when the government approached the court with its first request to approve a program involving what is now referred to as "bulk collection." In conducting this study, the Board was told by former FISA court judges that they were quite comfortable hearing only from government attorneys when evaluating individual surveillance requests but that the judges' decision-making would be greatly enhanced if they could hear opposing views when ruling on requests to establish new surveillance programs.

The classified and *ex parte* nature of the court's proceedings have raised concerns that it does not take adequate account of positions other than those of the government. But it is critical to the integrity of the court's process that the public have confidence in its impartiality and rigor. Therefore, the Board believes that some reforms are appropriate and would help bolster public confidence in the operation of the court. The most important reforms proposed by the Board are: (1) creation of a panel of private attorneys (or "Special Advocates") who can be brought into cases involving novel and significant issues by FISA court judges; (2) development of a process facilitating appellate review of FISA court decisions; and (3) increased opportunity for the FISA court to receive technical assistance and legal input from outside parties. We believe that our proposal successfully ensures the ability of the court to hear opposing views while not disrupting the court's operation or raising constitutional concerns about the role of the advocate.

Finally, our report discusses transparency — the tension between the competing imperatives of openness and secrecy, and the challenges of developing and implementing intelligence programs in ways that serve both values. Beyond the controversies that have arisen from the Section 215 and 702 programs, the Board believes that the government must take the initiative and formulate long-term solutions that promote greater transparency for government surveillance policies in order to inform public debate on technology, national security, and civil liberties. In this effort, all three branches have a role.

For the executive branch, disclosures about key national security programs that involve the collection, storage, and dissemination of personal information — such as the operation of the National Counterterrorism Center — show that it is possible to describe secret practices and policies publicly without damage to national security or operational effectiveness. With regard to the legislative process, even where classified intelligence operations are involved, the purposes and framework of a program for domestic intelligence collection should be debated in public. While some hearings and briefings may need to be conducted in secret during the process of developing legislation, to ensure that policymakers fully understand the intended use of a particular authority, the government should not base an ongoing program affecting the rights of Americans on an interpretation of a statute that is not apparent from a natural reading of the text. In the case of Section 215, for instance, the government should have made it publicly clear during the

reauthorization process that occurred in 2006 that it intended for Section 215 to serve as legal authority to collect data in bulk on an ongoing basis.

There also is a need for greater transparency in the operations of the FISA court. Prospectively, we encourage the judges on the court to continue the recent practice of writing opinions with an eye toward declassification, separating sensitive facts particular to the case at hand from broader legal analyses. The Board also believes that there is significant value in producing declassified versions of earlier FISA court opinions, and it recommends that the government undertake a classification review of all significant FISA court opinions and orders involving novel interpretations of law. We realize that the process of redacting opinions not drafted for public disclosure will be difficult and will burden individuals with other pressing duties, but we believe that it is appropriate to make the effort where those opinions and orders complete the historical picture of the development of legal doctrine regarding matters within the jurisdiction of the court. In addition, should the government adopt our recommendation for a Special Advocate in the FISA court, the nature and extent of that advocate's role must be transparent to be effective.

It is also important to promote transparency through increased reporting to the public on the scope of surveillance programs. The Board's report urges the government to work with Internet service providers and other companies to reach agreement on standards allowing reasonable disclosures of aggregate statistics that would be meaningful without revealing sensitive government capabilities or tactics. We note that the government recently announced an agreement with providers as a step in this direction. We recommend that the government should also increase the level of detail in its unclassified reporting to Congress and the public regarding surveillance programs.

V. The Board's Recommendations

Based upon the findings and analysis described above, the PCLOB has made twelve specific recommendations regarding the Section 215 telephone records program, the operation of the FISA court, and transparency in intelligence activities. Ten of those recommendations are unanimous, as discussed further below. The Board's recommendations can be summarized as follows.

Recommendation 1: The government should end its Section 215 bulk telephone records program.

The Section 215 bulk telephone records program lacks a viable legal foundation under Section 215, implicates constitutional concerns under the First and Fourth

Amendments, raises serious threats to privacy and civil liberties as a policy matter, and has shown only limited value. As a result, the Board recommends that the government end the program.

Without the current Section 215 program, the government would still be able to seek telephone calling records directly from communications providers through other existing legal authorities. The Board does not recommend that the government impose data retention requirements on providers in order to facilitate any system of seeking records directly from private databases.

Once the Section 215 bulk collection program has ended, the government should purge the database of telephone records that have been collected and stored during the program's operation, subject to limits on purging data that may arise under federal law or as a result of any pending litigation.

The Board also recommends against the enactment of legislation that would merely codify the existing program or any other program that collects bulk data on such a massive scale regarding individuals with no suspected ties to terrorism or criminal activity. Moreover, the Board's constitutional analysis should provide a message of caution, and as a policy matter, given the significant privacy and civil liberties interests at stake, if Congress seeks to provide legal authority for any new program, it should seek the least intrusive alternative and should not legislate to the outer bounds of its authority.

The Board recognizes that the government may need a short period of time to explore and institutionalize alternative approaches, and believes it would be appropriate for the government to wind down the 215 program over a brief interim period. If the government does find the need for a short wind-down period, the Board urges that it should follow the procedures under Recommendation 2 below.

***Recommendation 2*: The government should immediately implement additional privacy safeguards in operating the Section 215 bulk collection program.**

The Board recommends that the government immediately implement several additional privacy safeguards to mitigate the privacy impact of the present Section 215 program. The recommended changes can be implemented without any need for congressional or FISC authorization. Specifically, the government should:

(a) reduce the retention period for the bulk telephone records program from five years to three years;
(b) reduce the number of "hops" used in contact chaining from three to two;

(c) submit the NSA's "reasonable articulable suspicion" determinations to the FISC for review after they have been approved by NSA and used to query the database; and
(d) require a "reasonable articulable suspicion" determination before analysts may submit queries to, or otherwise analyze, the "corporate store," which contains the results of contact chaining queries to the full "collection store."

***Recommendation 3*: Congress should enact legislation enabling the FISC to hear independent views, in addition to the government's views, on novel and significant applications and in other matters in which a FISC judge determines that consideration of the issues would merit such additional views.**

Congress should authorize the establishment of a panel of outside lawyers to serve as Special Advocates before the FISC in appropriate cases. The presiding judge of the FISC should select attorneys drawn from the private sector to serve on the panel. The attorneys should be capable of obtaining appropriate security clearances and would then be available to be called upon to participate in certain FISC proceedings.

The decision as to whether the Special Advocate would participate in any particular matter should be left to the discretion of the FISC. The Board expects that the court would invite the Special Advocate to participate in matters involving interpretation of the scope of surveillance authorities, other matters presenting novel legal or technical questions, or matters involving broad programs of collection. The role of the Special Advocate, when invited by the court to participate, would be to make legal arguments addressing privacy, civil rights, and civil liberties interests. The Special Advocate would review the government's application and exercise his or her judgment about whether the proposed surveillance or collection is consistent with law or unduly affects privacy and civil liberties interests.

***Recommendation 4*: Congress should enact legislation to expand the opportunities for appellate review of FISC decisions by the Foreign Intelligence Surveillance Court of Review, and for review of those decisions by the Supreme Court of the United States.**

Providing for greater appellate review of rulings by the FISC and by its companion appellate court, the Foreign Intelligence Surveillance Court of Review ("FISCR"), will strengthen the integrity of judicial review under FISA. Providing a role for the Special Advocate in seeking that appellate review will further increase public confidence in the integrity of the process.

***Recommendation 5*: The FISC should take full advantage of existing authorities to obtain technical assistance and expand opportunities for legal input from outside parties.**

FISC judges should take advantage of their ability to appoint Special Masters or other technical experts to assist them in reviewing voluminous or technical materials, either in connection with initial applications or in compliance reviews. In addition, the FISC and the FISCR should develop procedures to facilitate amicus participation by third parties in cases involving questions that are of broad public interest, where it is feasible to do so consistent with national security.

***Recommendation 6*: To the maximum extent consistent with national security, the government should create and release with minimal redactions declassified versions of new decisions, orders and opinions by the FISC and FISCR in cases involving novel interpretations of FISA or other significant questions of law, technology or compliance.**

FISC judges should continue their recent practice of drafting opinions in cases involving novel issues and other significant decisions in the expectation that declassified versions will be released to the public. The government should promptly create and release declassified versions of these FISC opinions.

***Recommendation 7*: Regarding previously written opinions, the government should perform a declassification review of decisions, orders and opinions by the FISC and FISCR that have not yet been released to the public and that involve novel interpretations of FISA or other significant questions of law, technology or compliance.**

Although it may be more difficult to declassify older FISC opinions drafted without expectation of public release, the release of such older opinions is still important to facilitate public understanding of the development of the law under FISA. The government should create and release declassified versions of older opinions in novel or significant cases to the greatest extent possible consistent with protection of national security. This should cover programs that have been discontinued, where the legal interpretations justifying such programs have ongoing relevance.

***Recommendation 8*: The Attorney General should regularly and publicly report information regarding the operation of the Special Advocate program recommended by the Board. This should include statistics on the frequency and nature of Special Advocate participation in FISC and FISCR proceedings.**

These reports should include statistics showing the number of cases in which a Special Advocate participated, as well as the number of cases identified by the government as raising a novel or significant issue, but in which the judge declined to invite Special Advocate participation. The reports should also indicate the extent to which FISC decisions have been subject to review in the FISCR and the frequency with which Special Advocate requests for FISCR review have been granted.

> ***Recommendation 9*: The government should work with Internet service providers and other companies that regularly receive FISA production orders to develop rules permitting the companies to voluntarily disclose certain statistical information. In addition, the government should publicly disclose more detailed statistics to provide a more complete picture of government surveillance operations.**

The Board urges the government to pursue discussions with communications service providers to determine the maximum amount of information that companies could voluntarily publish to show the extent of government surveillance requests they receive per year in a way that is consistent with protection of national security. In addition, the government should itself release annual reports showing in more detail the nature and scope of FISA surveillance for each year.

> ***Recommendation 10*: The Attorney General should fully inform the PCLOB of the government's activities under FISA and provide the PCLOB with copies of the detailed reports submitted under FISA to the specified committees of Congress. This should include providing the PCLOB with copies of the FISC decisions required to be produced under Section 601(a)(5).**[22]

> ***Recommendation 11*: The Board urges the government to begin developing principles and criteria for transparency.**

The Board urges the Administration to commence the process of articulating principles and criteria for deciding what must be kept secret and what can be released as to existing and future programs that affect the American public.

> ***Recommendation 12*: The scope of surveillance authorities affecting Americans should be public.**

In particular, the Administration should develop principles and criteria for the public articulation of the legal authorities under which it conducts surveillance affecting

[22] Section 601(a)(5), which is codified at 50 U.S.C. § 1871(a)(5), requires the congressional intelligence and judiciary committees to be provided with decisions, orders, and opinions from the FISC, and from its companion appellate court, that include significant construction or interpretation of FISA provisions.

Americans. If the text of the statute itself is not sufficient to inform the public of the scope of asserted government authority, then the key elements of the legal opinion or other documents describing the government's legal analysis should be made public so there can be a free and open debate regarding the law's scope. This includes both original enactments such as 215's revisions and subsequent reauthorizations. While sensitive operational details regarding the conduct of government surveillance programs should remain classified, and while legal interpretations of the application of a statute in a particular case may also be secret, the government's interpretations of statutes that provide the basis for ongoing surveillance programs affecting Americans can and should be made public.

VI. Minority Views

While ten of the Board's twelve recommendations are unanimous, two are not. Board members Rachel Brand and Elisebeth Collins Cook did not join Recommendation 1 (that the government end its Section 215 bulk telephone records program) or Recommendation 12 (that the scope of surveillance authorities affecting Americans be made public). In addition, Ms. Brand and Ms. Cook did not join the Board's statutory or constitutional analysis. Both members explained their views in separate statements that are incorporated in the Board's report.[23]

Ms. Brand and Ms. Cook both reached a different judgment than did the Board majority about how the value of the program weighs against its implications for privacy and civil liberties. Ms. Brand stressed that the usefulness of the program "may not be fully realized until we face another large-scale terrorist plot against the United States or our citizens abroad," and that "if that happens, analysts' ability to very quickly scan historical records from multiple service providers to establish connections (or avoid wasting precious time on futile leads) could be critical in thwarting the plot."[24] Ms. Cook emphasized the value of a tool that allows investigators to "triage and focus on those who are more likely to be doing harm to or in the United States," "more fully understand our adversaries in a relatively nimble way," and "verify and reinforce intelligence gathered from other programs or tools."[25]

With respect to potential intrusions on privacy and civil liberties, Ms. Brand and Ms. Cook emphasized that the NSA does not acquire the contents of telephone calls or any personally identifying information about callers under this program, as well as the strict

---

23 *See* Separate Statement by Board Member Rachel Brand (Jan. 23, 2014) ("Brand Statement"), and Separate Statement by Board Member Elisebeth Collins Cook (Jan. 23, 2014) ("Cook Statement"), *available at* http://www.pclob.gov/. Both statements are included as annexes to the Board's report.

24 Brand Statement at 5-6.

25 Cook Statement at 4.

safeguards and limitations governing the NSA's *use* of the records it obtains. While agreeing that certain additional privacy safeguards nevertheless are warranted (spelled out in the Board's second recommendation), in their judgment the value of the program, with those safeguards in place, outweighs its intrusions on privacy and civil liberties. Ms. Brand, however, noted that "if an adequate alternative that imposes less risk of privacy intrusions can be identified, the government should adopt it,"[26] and Ms. Cook recommended that the Intelligence Community devise "metrics for assessing the efficacy and value of intelligence programs, particularly in relation to other tools and programs," as well as conduct periodic assessments to gauge the relative value of such programs.[27]

Ms. Brand and Ms. Cook also declined to join the Board's legal conclusion that the bulk telephone records program is unauthorized by Section 215 of the Patriot Act. They concluded that the government's interpretation of the statute is "at least a reasonable reading, made in good faith by numerous officials in two Administrations of different parties," as Ms. Brand put it,[28] representing "a good faith effort to subject a potentially controversial program to both judicial and legislative oversight," as Ms. Cook put it,[29] and stressed that the government's interpretation has been upheld by numerous Article III judges.

With respect to Recommendation 12 (regarding transparency in the scope of surveillance authorities affecting Americans), Ms. Brand explained that she does not believe "that an intelligence program or legal justification for it must necessarily be known to the public to be legitimate or lawful."[30] Ms. Cook similarly expressed her view that in a representative democracy "it is simply not the case that a particular use or related understanding of a statutory authorization is illegitimate unless it has been explicitly debated in an open forum."[31]

While the majority of the Board did not obtain unanimity on these two recommendations (among twelve recommendations overall), it believes that the reasoned and transparent disagreement on those points reflected in the Board's report and its minority statements can assist the Administration, Congress, and the public as they debate the future of our nation's surveillance practices.

---

26 Brand Statement at 6.
27 Cook Statement at 4.
28 Brand Statement at 3.
29 Cook Statement at 2.
30 Brand Statement at 2.
31 Cook Statement at 4.

VII. Conclusion

Thank you for the opportunity to testify before the House Judiciary Committee today regarding the Board's report. As already noted, the Board welcomes the opportunity for further dialogue within the executive branch and with Congress about the issues raised in its report and how best to implement the Board's recommendations.