Center for a New American Security

Written Statement for the Privacy and Civil Liberties Oversight Board Public Forum on February 8, 2019, to Examine Emerging Issues in Countering Terrorism and Protecting Civil Liberties

Carrie Cordero, Robert M. Gates Senior Fellow, Center for a New American Security

Introduction

Thank you to the Chairman and Board members for the invitation to join this first public forum of the newly reconstituted Board. I would like to add a special note of thanks to former chair of the Privacy and Civil Liberties Oversight Board (PCLOB or the Board) Elisebeth Collins and to the Board's current and former professional staff for keeping it afloat during a lengthy period of uncertainty and delay. I am pleased that the President has nominated, and the Senate confirmed, the three Board members present today, and look forward to the Board reaching its full complement.

The Board's work is important both for the substance on which it engages and also for the transparency that it provides to the public. It has attained a valued role in the privacy community as well as in the intelligence community. And those are not two entirely distinct, separate entities. This Board will be working with an intelligence community that has taken significant steps forward in developing a network of privacy professionals inside the community. Having myself recently participated in the intelligence community's annual privacy, civil liberties, and transparency officers' conference, I feel comfortable in reporting that the intelligence community has institutionalized several of its transparency initiatives that have been developed over the past five plus years, so that they have largely continued on track, despite changes in political leadership. That is as it should be.

The Board's Role

As you know, the previous iteration of the Board was heavily invested in two major bodies of work, the reports on the 215 program and on Section 702 acquisition, both conducted under the Foreign Intelligence Surveillance Act (FISA). These were timely and valuable contributions to the public debate over surveillance authorities. They were also after-the-fact reviews and reports. They were necessarily reactionary. I am hopeful that the next iteration of the Board's work may permit you to more regularly use two particular tools available in your toolkit:

First, the advisory role. When at all possible, the Board's engagement on the front end of collections using new technologies can be a productive use of the Board's time. While not as public-facing because it takes place behind the scenes, to any extent you can get in on the front end of activities – particularly those that apply new technologies or large datasets affecting privacy interests – before the procedures are rolled out and the workforce trained on them, the better.

Second, legislation consultation. One of the most important lessons from the scholarly and public reaction to the Snowden disclosures was, in addition to the need for greater transparency about the legal interpretations, the law must be clearer itself. The Board can play a useful role in legislative consultation if it eyes proposed legislation from the perspective of whether the text permits activities that are probably only clear to those with inside or classified knowledge of how

1152 15th Street NW
Suite 950
Washington, DC 20005

CNAS.org / @CNASdc
T: 202.457. 9400
F: 202.457.9401

surveillance law works. Is proposed legislation too opaque, even to the informed outside observer? This is a question that the Board is well positioned to provide advice to executive branch agencies and policymakers on when requests for new authorities regarding counterterrorism activities are being drafted or proposed.

With respect to the Board's consideration of its substantive agenda going forward, I offer the following observations:

I. Privacy Implications of Leaks and Hacks

The Board should take under consideration the privacy implications of leaks and hacks and conduct oversight over the government's responsibilities, policies, procedures, and practices to secure private information obtained during counterterrorism investigations and activities. Despite policies intended to address information safeguarding, we are all aware that there have been substantial leaks of classified information over the course of nearly a decade now.

The unauthorized disclosure and subsequent publication of materials facilitated by Chelsea Manning was in 2010. The Snowden disclosures began in the summer of 2013. Both were high volume leaks of sensitive government data.[1] In addition, of national security significance, but perhaps less relevant to privacy considerations, is that intelligence community elements have experienced the unauthorized disclosure of classified information concerning sensitive hacking tools.[2]

More broadly across government, the OPM hack exposed not only millions of Americans' information but the weakness of non-national security–related government data storage. And outside government, releases of information that were facilitated by hostile foreign interests during the course of the 2016 election have implicated privacy interests of Americans, including the content of emails. Further, various categories of Americans' data have been stolen and/or exposed as a result of unauthorized access to private sector networks.

The portrait that emerges is one of Americans' data constantly being not protected or secured across a wide swath of domains. This persistent era of leaks and hacks presents special challenges for collection of large volumes of data on Americans collected in the counterterrorism

---

[1] A different type of unauthorized disclosure took place circa February 2017, when the substance of a conversation between Russian Ambassador Sergey Kislyak and then-National Security Advisor Michael Flynn was disclosed to the media. While not precisely a privacy issue (assuming that the conversation at issue took place on a government device or phone line), this disclosure should be on the radar of privacy and civil liberties oversight officials given that it involved the unauthorized disclosure of the content of communications.

[2] *United States v. Joshua Adam Schulte*, S1 17 Cr. 548, superseding indictment, https://www.justice.gov/usao-sdny/press-release/file/1072871/download; "Joshua Adam Schulte Charged With The Unauthorized Disclosure of Classified Information And Other Offenses Relating To the Theft of Classified Material From the Central Intelligence Agency," United States Department of Justice, press release, June 18, 2018, https://www.justice.gov/usao-sdny/pr/joshua-adam-schulte-charged-unauthorized-disclosure-classified-information-and-other; Adam Goldman, "New Charges in Huge CIA Breach Known as Vault 7," *The New York Times*, June 18, 2018, https://www.nytimes.com/2018/06/18/us/politics/charges-cia-breach-vault-7.html; and Greg Otto, "Accused Vault 7 Leaker to Face New Charges," *Cyberscoop*, November 1, 2018, https://www.cyberscoop.com/joshua-schulte-vault-7-new-charges/.

context, both international terrorism and domestic terrorism, given that the Board's mandate is not limited to one or the other.

Based on the pervasive nature of the threat of exposure of sensitive information, including the content and metadata of Americans and other persons whose communications are incidentally collected pursuant to lawful collection authorities, procedures and practices governing databases containing large volumes of information should be reviewed for both the:

- privacy nature of the information, and
- security measures that the intelligence community or other relevant agencies are applying commensurate with the type of information retained and the risk of exposure.

Generally speaking, there are three ways sensitive data can make its way out of its secure location: unauthorized disclosures (leaks), malicious cyber activity (hacks), and inadvertent exposure (glitches or spillage). Based on the persistent nature of the disclosures the community has experienced, security of privacy-implicated information should be on the Board's agenda. This proposed work is within the scope of the Board's mandate, including its role in the development of information sharing guidelines. The effort should include analysis of how content from signals intelligence is stored and whether existing security measures are adequate.[3] In the age of leaks and hacks, security of data collected is a privacy issue. Sensitive information that cannot reasonably be protected should be given greater scrutiny as to whether its continued collection and retention is appropriate from a civil liberties, privacy, and national security perspective.

II. Retention Periods for Counterterrorism Information

As a corollary to the Board directing attention to the security of information collected and retained, the Board should conduct:

- a review of retention procedures and implementation;
- comparison of retention periods for similar or the same data across agencies, for consistency as it relates to privacy protection;
- age off rules and practices;
- compliance with existing age off, deletion, and data segregation practices; and
- a review of processes for verifying data deletion.

In short, exposures since 2010 have changed the analysis on retention. From time to time, I am asked where my views have changed on surveillance law and policy since leaving government service in 2010. I remain comfortable that strong legal authorities for protecting the nation are critical.

---

[3] Intelligence Community Directive (ICD) Number 501, Discovery and Dissemination or Retrieval of Information Within the Intelligence Community, (2009). Executive Order 13587, Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information (2011). Guidelines to Ensure that the Information Privacy and Other Legal Rights of Americans Are Protected in the Development and Use of the Information Sharing Environment (2006) ("Each agency shall use appropriate physical, technical, and administrative measures to safeguard protected information shared through the ISE from unauthorized access, disclosure, modification, use, or destruction.")

Where my views have shifted some, to keep up with current developments, are on retention periods and risks of collection if the information cannot be protected. What has changed the most since my tenure in government service is a pervasive and unabated environment of leaks and hacks.

With respect to retention, I would encourage the Board to look at, but also beyond, information collected under FISA. The prior Board necessarily spent substantial time on FISA-related collection. While collection under FISA is important to the Board's work, FISA is highly regulated and has well-developed interagency oversight and compliance mechanisms, as well as court supervision and compliance monitoring. Agencies' retention of counterterrorism information not governed by FISA is worth analyzing because there are not the same oversight and compliance mechanisms. The Board might be interested in understanding what of the other information collected is information that has privacy implications.

III. December 2019 Sunsets

As the Board members are aware, there are three provisions of FISA set to sunset at the end of this year, unless reauthorized:

- Roving wiretaps;
- The "lone wolf" provision; and
- Section 215, or business records, provision.

Of most interest to the Board should be the Section 215 authorization.

As previously noted, an important lesson of 2013 was that reasonably informed observers should understand what the law authorizes. The Board could take a constructive role by reviewing how the USA Freedom Act amendments to the acquisition of call records has been implemented and making recommendations to amendments to the law, if appropriate, if there are significant discrepancies between the text and the implementation in practice. Given that the collection of this information has been fully exposed publicly, there seems little upside and significant downside in having ambiguities about how the law is being used.

In addition, a question for further inquiry is whether the process contemplated by the USA Freedom Act is working as intended. In the summer of 2018, the NSA publicly revealed that companies were providing data beyond the scope of what was authorized. Ultimately, the compliance issue resulted in significant data deletion, calling into question the efficacy of the collection activity.[4] Given the upcoming sunset at the end of this year, the PCLOB can play a constructive role informing the debate.

Thank you for the opportunity to provide these views to the Board.

[4] Robert Chesney, *Three FISA Authorities Sunset in December: Here's What You Need to Know,* Lawfare, January 16, 2019.