KNIGHT
FIRST AMENDMENT
INSTITUTE
at Columbia University

PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD

Public Hearing on Oversight Agenda for 2019 and Beyond
February 8, 2019

Submission of Alex Abdo
Senior Staff Attorney
Knight First Amendment Institute
at Columbia University

Thank you for the opportunity to testify before the Privacy and Civil Liberties Oversight Board as it considers its oversight agenda for 2019 and beyond. The Board has contributed significantly to public understanding of the activities of the intelligence agencies, and I commend the Board for hosting this session. Before addressing the Board's agenda, I want to encourage whatever efforts are being made to fill the Board's vacancies. The Board's legitimacy and its ability to operate effectively depend on its being fully staffed in a bipartisan manner, and so I hope the Board reaches full capacity again, soon.

With respect to the Board's agenda, I would like to make one proposal: the Board should make it an explicit part of its agenda to narrow the gaps between what the public believes the intelligence agencies are doing and what the agencies are actually doing. The Board is uniquely well-positioned to identify these gaps and to advocate for the declassification of information sufficient to allow the public to understand, in at least general terms, the legal authorities of the intelligence agencies and the activities said to be justified by them. As I'll explain below, this sort of transparency would promote democratic self-government, the legitimacy of the Board, and the legitimacy of the intelligence agencies' activities.

* * *

Since the reforms put in place following the investigations of the Church and Pike Committees in the 1970s, the system of oversight of the intelligence agencies has been based upon a fragile premise. Secret

oversight is sufficient, we have been told, because the officials who oversee the agencies have access to classified information, and because these officials are ultimately accountable to the public.

Six years ago, the fragility of that premise was exposed in dramatic fashion. In June 2013, reporters working with documents supplied by Edward Snowden began to report on classified programs of mass surveillance. Although those programs had been reviewed and approved in secret by members of all branches of government, they had outgrown the public's understanding of what the intelligence agencies were permitted and able to do. When these programs were exposed, many Americans were surprised and even shocked. As Senator Ron Wyden had predicted with respect to at least one of the programs revealed, "When the American people find out how their government has secretly interpreted the Patriot Act, they will be stunned and they will be angry."[1] He was right.

In response to these revelations, the government officially acknowledged certain aspects of some of these surveillance programs, and Americans were for the first time able to have an informed discussion about some of the intelligence agencies' surveillance authorities. That debate culminated in a pitched legislative battle over competing proposals to substantially reform our foreign intelligence surveillance laws.

One key lesson of the Snowden revelations is that secret oversight is not a substitute for transparency or for the public debate that transparency makes possible. Some measure of transparency is necessary to ensure that the public understands, in at least general terms, the legal authorities of the intelligence agencies and the activities said to be justified by those authorities. Absent that level of transparency, gaps will inevitably develop between the agencies' authorities and activities, on the one hand, and the public's understanding of those authorities and activities, on the other.

These gaps are corrosive. They deprive the public of the opportunity to understand, endorse, or object to the agencies' activities, and they thereby disconnect the agencies' activities from the democratic consent

---

[1] Sen. Ron Wyden, *Statement on Patriot Act Reauthorization* (May 26, 2011), https://www.wyden.senate.gov/news/press-releases/in-speech-wyden-says-official-interpretations-of-patriot-act-must-be-made-public.

that should underwrite them. They deprive the agencies' activities of democratic legitimacy, and they feed public skepticism and distrust of the agencies themselves.

Many others have recognized that the Snowden disclosures exposed a failure in transparency and democratic oversight. In a speech delivered to the University of Virginia School of Law in 2015, Jack Goldsmith said: "The American people, and the rule of law, can accept secrecy about NSA operations, and sources, and compliance rates with generally known authorities. But it is unacceptable when the contours of a massive governmental surveillance operation in the United States are unknowable to the public and a huge surprise based on known legal authorities."[2] James Clapper, the former Director of National Intelligence, recognized the same when he argued that the public backlash against the NSA's overreaching surveillance was due in part to the NSA's excessive secrecy. Had the NSA been open with the public, he opined, "[w]e wouldn't have had the problem we had."[3] Transparency, in other words, is essential to the legitimacy of the intelligence agencies' activities.

What I hope to underscore today is that *the Board*, in particular, has a crucial role to play in striking the right balance between the secrecy necessary to the work of the intelligence agencies and the transparency necessary for democratic accountability and legitimacy. The Board should embrace transparency as a key aim of its work. In every area of its oversight, the Board should push for declassification of the information necessary for the public to understand the intelligence agencies' authorities and activities in at least general terms.

The Board is uniquely well-positioned within government to push for this transparency. As an independent body meant to ensure that our nation's intelligence activities are consistent with our commitment to civil liberties, the Board has a singular vantage point. It has the access needed to receive briefings by the intelligence agencies on the harms they believe would flow from the disclosure of information about their activities. It has the independence necessary to consider the harms to our

---

[2] Jack Goldsmith, *The Rule of Law in Secret* (Apr. 2, 2015), http://jackgoldsmith.org/the-rule-of-law-in-secret/.

[3] Eli Lake, *Spy Chief: We Should've Told You We Track Your Calls*, Daily Beast, Feb. 17, 2014, https://www.thedailybeast.com/spy-chief-we-shouldve-told-you-we-track-your-calls.

democracy that would flow from the *failure* to disclose information about those activities. And it has a mandate from Congress to "[i]nform[] the public" by making its reports "available to the public to the greatest extent that is consistent with the protection of classified information."[4]

Historically, the intelligence agencies have not shown the ability to fairly balance the interests of secrecy and transparency. In weighing the risks of disclosure against the harms of secrecy, the agencies tend to overestimate the former and underestimate the latter. This is in part because the legal and professional incentives within the intelligence agencies all tilt steeply toward secrecy. Officials risk punishment for disclosing information that causes harm, but not for suppressing information whose disclosure would serve the public interest. The imbalance between these incentives is one reason that nearly every senior official to leave government and discuss the subject has complained about rampant over-classification.

The Board, on the other hand, has already shown its ability to balance these interests more evenhandedly. In its report on Section 702 of the Foreign Intelligence Surveillance Act, the Board noted that it had prevailed upon the executive branch to declassify facts necessary for greater public understanding of Section 702 surveillance:

> In the preparation of this Report, the Board worked with the Intelligence Community to seek further declassification of information related to the Section 702 program. Specifically, the Board requested declassification of additional facts for use in this Report. Consistent with the Board's goal of seeking greater transparency where appropriate, the request for declassification of additional facts to be used in this Report was made in order to provide further clarity and education to the public about the Section 702 program. The Intelligence Community carefully considered the Board's requests and has engaged in a productive dialogue with PCLOB staff. The Board greatly appreciates the diligent efforts of the Intelligence Community to work through the declassification process,

[4] 42 U.S.C. § 2000ee(f)(1).

> and as a result of the process, many facts that were previously classified are now available to the public.[5]

I recognize that few would dispute the importance of transparency, and that the difficulty lies in applying that abstract value to specific facts. Here, it might make sense for the Board to articulate factors it will consider when deciding whether to advocate for greater transparency. Those factors might include: (1) whether a secret intelligence activity has broad implications for individual rights, (2) whether a secret intelligence activity involves the use of a novel or transformative capability (such as facial recognition, artificial intelligence, bulk collection, or bulk analysis), (3) whether the likelihood of, or the harm that would flow from, abuse of a particular intelligence capability is high, (4) whether a secret intelligence activity is based upon an unusual or unintuitive interpretation of law, (5) whether a secret intelligence activity relies upon an interpretation of law about which there is conflict among the courts, or (6) whether there is any other reason to believe that the public would be surprised to learn of a particular intelligence activity or authority.

By embracing an agenda of transparency in this way, the Board would promote the values of self-government and democratic legitimacy, as I discussed earlier. The Board would also promote at least two other important interests.

First, by embracing an agenda of transparency, the Board would make its own work more effective and more legitimate. To date, the work of the Board has been received positively by the public due in large part to the transparency with which it has been able to operate. Although the Board deals largely in classified information, the Board has held open hearings, received unclassified testimony, and issued five oversight reports publicly. This transparency has allowed the public to read the Board's conclusions, to weigh the underlying evidence, and to reach its own determinations. It has also allowed courts, in the handful of cases where relevant, to better understand the activities of the intelligence agencies. As a result, the Board has established trust and credibility with civil society and the public more broadly.

---

[5] *See* PCLOB, *Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act* at 3 (July 2, 2014), https://www.pclob.gov/library/702-Report-2.pdf.

But absent a significant change, the Board soon may no longer be able to operate as transparently. The Board has been able to operate with relative transparency thus far primarily due to the official acknowledgments the government has made in response to the Snowden revelations. But those disclosures were an aberration. Now, nearly six years removed from the Snowden revelations, we are receiving very little new information. The government has declassified relatively little, for example, about the surveillance it carries out abroad under Executive Order 12,333, and even less about the ways in which it is exploiting new surveillance technologies.

Absent a concerted push to declassify more about the intelligence authorities and activities that the Board intends to review in the coming years, the Board will likely operate mostly behind closed doors. If the Board accepts that state of affairs, it will risk undermining its legitimacy and effectiveness as an overseer.

Second, by embracing an agenda of transparency, the Board would reduce the incentive of whistleblowers to leak classified information. Following the Snowden disclosures, many debated the circumstances in which leaking is justified. This is not an easy question, but surely one way to make leaking less likely is to make it less necessary. Snowden and others who have provided classified information to the press have described being motivated by a belief that the public would not approve of what it did not know was taking place in its name. That gap between public understanding and the intelligence agencies' actual practices creates a pressure that whistleblowers and leakers have tried to relieve. The pressure builds over time to the point when leaks appear to be the only safety valve. Working together, the Board and the intelligence agencies can minimize the incentive to leak through preventative and responsible release of the information necessary for the public to know, at least in general terms, what the agencies are doing.

How would the Board prioritize an agenda of transparency? It is necessarily difficult for someone without access to classified information to identify the largest gaps between public understanding and the actual authorities and activities of the intelligence activities. The Board would need to identify most of those gaps on its own or in consultation with others who have clearance, such as the panel of amici serving the Foreign Intelligence Surveillance Court, or the privacy officers and inspectors general within the intelligence agencies. This said, below is a partial list of gaps in public knowledge about the intelligence agencies' activities

that the Board should consider addressing as part of a transparency agenda.

1. *The number of U.S. persons swept up in foreign intelligence surveillance.* Remarkably, the intelligence agencies have not disclosed an estimate of the number of U.S. persons whose communications or metadata are swept up in the course of foreign intelligence surveillance directed at foreigners abroad. That estimate is crucial to understanding the effect of that surveillance on the rights of U.S. persons and on the reasonableness of the measures the intelligence agencies take to limit the collection, use, and retention of U.S. persons' data.

2. *The extent of foreign intelligence surveillance of journalists, dissidents, and others not engaged in wrongdoing.* Although the government often defends its foreign intelligence surveillance authorities as important tools in its effort to detect and prevent terrorism, the reality is that the authorities sweep far more broadly. Section 702 and Executive Order 12,333, in particular, permit surveillance targeting any non-U.S. person abroad thought to be communicating foreign intelligence. The extent of the government's use of its surveillance authorities to target journalists, dissidents, and others not engaged in wrongdoing is not known. Nor is it publicly known whether surveillance of such individuals represents a significant portion of the government's foreign intelligence surveillance efforts.

3. *The implications of* Carpenter v. United States *for other forms of surveillance.* In 2018, the Supreme Court held that law enforcement's collection of seven days' of cell site location information constitutes a "search" for purposes of the Fourth Amendment. The reasoning of the case calls into question the government's broader reliance on the third-party doctrine to justify the warrantless and large-scale collection of digital data. What impact the ruling has had on other forms of surveillance conducted by the intelligence agencies, however, is unknown.

4. *The limitations on surveillance imposed by the First Amendment.* A variety of surveillance statutes explicitly forbid the government from deploying certain surveillance techniques on the basis of activity protected by the First Amendment. Those statutory exemptions, however, are typically drawn very narrowly. For example, the business-records provision of the Foreign Intelligence Surveillance

Act provides that an investigation "shall . . . not be conducted of a United States person *solely* upon the basis of activities protected by the first amendment."[6] It is not publicly known how the intelligence agencies interpret these various statutory limits or, indeed, the limits imposed by the First Amendment itself, on their surveillance authority.

5. *The disparate impact of surveillance.* There is a widespread perception that today, as in the past, the burdens of surveillance fall most heavily on communities of color. The intelligence agencies, however, do not appear to conduct civil rights auditing of their surveillance activities, and so it is difficult for the public to know the extent of this disparate impact.

6. *Social media surveillance at the border.* Later this year, the State Department is expected to begin requiring all visa applicants to disclose their social media handles on their visa applications. The move carries troubling implications for First Amendment freedoms. Little is publicly known, however, about the manner in which the State Department intends to monitor or analyze the social media posts of visa applicants or of others connected to the applicants, to what end it intends to do so, or for how long.

7. *The use of other novel and invasive surveillance technologies.* Recent advances in technology enable new and invasive forms of surveillance. The extent to which the intelligence agencies have exploited those new technologies, in what ways, and with what impact on civil rights and civil liberties, is not known but essential to public understanding of the agencies' activities. For example, it is not known whether the intelligence agencies rely on artificial intelligence or machine learning to perform sophisticated analysis of the enormous volumes of data they collect. If so, it is of course not known how the agencies rely on such techniques. For example, do the agencies rely on machine-learning algorithms to algorithmically select new surveillance targets? Do the agencies' machine-learning algorithms reflect the human biases of their training data, as has been the case with publicly studied machine-learning algorithms?

[6] 50 U.S.C. § 1861(a)(2)(B) (emphasis added).

8. *The prioritization of security versus surveillance*. In November 2017, the White House issued a new policy to govern the Vulnerabilities Equities Process, which is the mechanism by which the government decides whether to disclose security vulnerabilities it has discovered (so that software firms can fix those flaws) or to retain those vulnerabilities (so that the intelligence agencies can exploit them to conduct surveillance). Although the policy was an improvement, it left important questions unanswered, including the precise scope of vulnerabilities covered by the process, the handling of vulnerabilities learned of through "partner agreements," and the breadth of the exceptions for misconfigured devices.

9. *The ways in which information acquired through foreign intelligence surveillance is accessed and used in criminal and immigration investigations*. While it is known that the Federal Bureau of Investigation searches certain repositories of information acquired through foreign intelligence surveillance in aid of its criminal investigations, the full extent of law-enforcement access and use of that information is not publicly known. For example, the public has little information about the ways in which such information is accessed and used by the Bureau or by Immigration and Customs Enforcement in ordinary investigations, or the policies that guide when that use is disclosed to criminal defendants or individuals whom the government seeks to deport.

Thank you, again, for the opportunity to submit this testimony. I look forward to answering any questions the Board has.