Statement of Chris Calabrese
Vice President, Policy
Center for Democracy & Technology

U.S. Privacy and Civil Liberties Oversight Board Public Forum
on

Countering Terrorism While Protecting Privacy and Civil Liberties: Where Do We Stand in 2019?

Ronald Reagan Building, Washington, DC

February 8, 2019

Chairman Klein and Members Felten and Nitze:

Thank you for the opportunity to testify on behalf of the Center for Democracy & Technology (CDT). CDT is a nonpartisan, nonprofit technology policy advocacy organization dedicated to protecting civil liberties and human rights, including privacy, free speech and access to information.[1] We applaud the Privacy and Civil Liberties Oversight Board (PCLOB) for holding this public forum on the current state of affairs of civil liberties and privacy in the fight against terrorism, which is of course central to PCLOB's mission.

Today I will discuss the important role that PCLOB plays in this area, and I will encourage PCLOB to focus on four initiatives:
(i) oversight of counterterrorism surveillance conducted under Executive Order 12333 (E.O. 12333);
(ii) promoting disclosures related to reauthorization of Section 215 of the USA PATRIOT Act;
(iii) investigating use by the Intelligence Community (IC) of data sets obtained from the private sector; and
(iv) misuse of counterterrorism authorities for domestic surveillance, such as surveillance of groups like Black Lives Matter.

Background

PCLOB's enabling statute gives it a critically important role in the fight against terrorism. It must: (a) analyze and review actions of the executive branch to protect the U.S. from terrorism, and ensure that the need for such actions is balanced with the need to protect privacy and civil liberties; and (b) ensure that liberty concerns are appropriately considered in the development and implementation of counterterrorism laws, regulations and policies.[2]

Congress also specifically tasked PCLOB with informing the public by making its reports public (while protecting classified information) and by holding public hearings and otherwise informing the public of its activities.[3] When it has enjoyed a quorum, PCLOB has played this role well. For example, PCLOB's investigation of the use of Section 702 of the Foreign Intelligence Surveillance Act (FISA) resulted in declassification of over 100 facts and rare praise for declassification efforts from the Federation of American Scientists Project on Government Secrecy.[4] Though we thought PCLOB's recommendations to rein in that surveillance came up short, the report and the facts disclosed in connection with development of the report informed the public debate on reauthorization of Section 702. We encourage you to continue to promote such disclosures because they help level the

[1] PCLOB Board Member Ed Felten sits on the CDT Board of Directors as does PCLOB nominee Travis LeBlanc.
[2] 42 U.S.C. 2000ee. https://www.pclob.gov/library/42USC2000ee-PCLOB_Enabling_Statute-3.pdf.
[3] Id.
[4] *Secrecy News,* July 28, 2014, *citing* statement of PCLOB Chairman David Medine at PCLOB's July 2, 2014 hearing. https://fas.org/sgp/news/secrecy/2014/07/072814.html. *Secrecy News* inquired about the facts declassified and received this very helpful response: https://fas.org/irp/eprint/pclob702-declass.pdf.

playing field for policy debates about counterterrorism activities and can result in better policy making.

We also encourage you to look for ways to be more transparent about how successful PCLOB has been in executing its "advice" function. PCLOB's enabling statute requires it to advise the President and Executive Branch agencies about ways to balance proposals to enhance government power with privacy and civil liberties, and to ensure oversight and supervision of such powers.[5] While protecting classified information, PCLOB should, as it did in August of 2014[6], publish a list of its short-term agenda items and include in that list specific mention of the subjects with respect to which it intends to offer advice, even if it does not intend to issue a full report on the activity with respect to which it offers advice. It should also let the public know the extent to which its advice has been adopted, partially adopted, or rejected. It has prominently reported such information on the recommendations it has made in its major reports,[7] but not on the advice function. For example, PCLOB's December 2018 semi-annual report discloses that it "provided advice on the first-ever procedures governing the dissemination of raw signals intelligence by the NSA."[8] To what extent was that advice adopted? The report is silent. In short, when your recommendations are adopted, take a victory lap; when they are rejected, let the public and Congress know so that other oversight tools can be brought to bear.

We understand that there are limits on PCLOB. It was hobbled for 20 months in 2017-18 when it lacked a quorum because the President and Congress were slow to replace PCLOB members who left or whose terms expired. Today, only 3 of your 5 members have been confirmed, and we were heartened this week to see that the Senate Judiciary Committee held hearings on confirmation of the other two members.[9] PCLOB has limited resources compared with the scope of its oversight duties. Its 16 employees (currently) are charged with overseeing the counterterrorism activity of an intelligence community comprising 17 agencies and hundreds of thousands of employees and contractors. Its roughly $8 million budget pales in comparison to the $60 billion budget of the IC. You have to pick your battles. We get that. Here are four battles worth picking:

PCLOB and Surveillance Under E.O. 12333

We urge you to complete, and release publicly, reports on E.O. 12333 activities on which substantial progress was made before PCLOB lost its quorum in January of 2017. E.O. 12333 authorizes broad surveillance for terrorism and other intelligence purposes. It is

---

[5] Id.
[6] PCLOB announces its short term agenda, August 7, 2014.
https://www.pclob.gov/newsroom/20140807.html
[7] For example, PCLOB reports about the extent to which the recommendations it has made about Sections 702 and 215 have been implemented. https://www.pclob.gov/reports/2016-update-on-215-702/
[8] PCLOB Semi-Annual Report, December 2018, p. 8.
https://www.pclob.gov/library/Semi-Annual%20Report%20-%20PCLOB%20Dec%202018.pdf
[9] Senate Judiciary Committee notice of hearings on nominations, February 5, 2019.
https://www.judiciary.senate.gov/meetings/02/05/2019/nominations.

much broader than the surveillance permitted in the United States under FISA. For example, as a result of the USA FREEDOM Act, FISA surveillance in the U.S. must be targeted; surveillance directed at foreigners abroad under E.O. 12333 can be conducted in bulk. The permitted purpose of surveillance under E.O. 12333 is quite broad, encompassing all activities and intentions of non-U.S. persons.[10] This broad authority has resulted in broad surveillance programs, including "Co-Traveler", through which the U.S. captured billions of location updates daily from mobile phones around the world, and "Muscular", through which the NSA intercepted all data transmitted between certain Google and Yahoo! data centers outside the U.S.[11]

PCLOB reported that it was doing three in-depth examinations of certain activities conducted under E.O. 12333. One "deep dive" related to activities of the NSA, and two related to activities at the CIA. PCLOB's December 2018 semi-annual report indicates that one of the CIA deep dives concluded with a classified report from the PCLOB in January 2017, and that the other two reports had not yet been completed. [12] We urge you to seek declassification of as many facts as possible related to the completed E.O. 12333 deep dive on particular CIA activities, and to release a declassified version of your report. We also ask that you complete the other two E.O. 12333 deep dives that were in the works, and that you go through a similar process of declassification and release of the reports on those activities as well.

PCLOB and Section 215 Surveillance

We ask that you undertake the following with respect to Congress' consideration of reauthorizing surveillance under Section 215 of the USA PATRIOT Act:
(i) inform the public of the approximate number of unique identifiers involved in the call detail records (CDR) program, or provide assistance to the IC in developing such approximation;
(ii) explain how surveillance of 42 targets under this program generated 151 million call detail records in 2016, and surveillance of only 40 targets under this program generated 534 million CDRs in 2017, and make recommendations about what could be done to mitigate this enormous privacy risk;
(iii) report publicly on the nature of the mistake that caused the NSA to unlawfully collect CDRs under this authority and dispose last year of all the CDRs it had collected because it couldn't distinguish the lawfully collected CDRs from those that were unlawfully collected; and

---

[10] E.O. 12333 Section 3.5(e) defines the permitted foreign intelligence purpose of surveillance under E.O. 12333 to include collection of "information relating to the capabilities, intentions or activities of … foreign persons." https://www.dni.gov/index.php/ic-legal-reference-book/executive-order-12333.
[11] *See*, *Secret Surveillance: Five Large-Scale Global Programs,* a May 2015 submission of CDT and the American Civil Liberties Union to the U.N. Human Rights Council in connection with the 22nd Session of the Universal Periodic Review Working Group. https://cdt.org/files/2014/09/cdt-aclu-upr-9152014.pdf .
[12] PCLOB Semi-Annual Report, December 2018, p. 7.
https://www.pclob.gov/library/Semi-Annual%20Report%20-%20PCLOB%20Dec%202018.pdf.

(iv) look behind, and if necessary, de-bunk any governmental claims of efficacy of surveillance under Section 215.

These requests are time-sensitive: Section 215 will expire on December 15, 2019, unless Congress acts, and we expect congressional action to begin in earnest this summer.

Section 215 of the USA PATRIOT Act authorized the government to demand any "tangible thing" – including business records – relevant to a foreign intelligence investigation not concerning a U.S. person, or an investigation to protect against international terrorism or clandestine intelligence activities.[13] The NSA used this authority to collect, in bulk, records of phone calls to, from, and within the United States, including prospective records. When this activity was disclosed in 2013, Congress passed the USA FREEDOM Act, which outlawed bulk collection of metadata in the U.S. under any intelligence authority including Section 215, and established authority for the IC to make targeted demands on U.S. telecoms for call detail records (CDRs). To make such a demand, the IC must establish to the FISA Court that there is a "reasonable articulable suspicion" that the target's selector (a phone number or a device identifier) is associated with a foreign power or agent of a foreign power engaged in international terrorism or activities in preparation therefor.[14] Under the terms of the statute, the government could then demand records of phone calls to or from the selector as well as records of phone calls to or from those who had communicated with the target using the targeted selector.

The USA FREEDOM Act requires the government to disclose the number of unique identifiers involved in the CDR program. This figure would give the public a good grasp of the scope of the program. It would help people understand the likelihood that records of their own calls were or were not being collected. However, the IC has failed to disclose this number – even after pledging that it would – citing the difficulty of calculating it or even of estimating it. We are asking you to look behind this claim and assist the IC in developing and disclosing this information or an approximation.

In addition, small numbers of targeted selectors are generating huge numbers of CDRs going into governmental databases. Why was there a threefold jump in these numbers from one year to the next, even though the number of targets declined? Is the collection of 534 million CDRs actually necessary for this program to be effective, or could many of the records – perhaps the "second hop" records – be eliminated?

On June 28, the NSA reported that it was deleting hundreds of millions of CDRs it collected under Section 215 because some had been collected unlawfully, and it could not separate the lawfully collected CDRs from the unlawfully collected CDRs.[15] Though PCLOB lacked a quorum at the time, notice of this deletion was sent to it. While we applaud the NSA for its decision to delete data in this circumstance, its failure to explain the "technical

[13] 50 U.S.C. 1861. https://www.law.cornell.edu/uscode/text/50/1861
[14] 50 U.S.C. 1861(b)(2)(C)(ii).
[15] NSA Reports Data Deletion, June 28, 2018.
https://www.nsa.gov/news-features/press-room/Article/1618691/nsa-reports-data-deletion/.

irregularities" that resulted in this unlawful collection undermine confidence in the program and in the NSA's ability to administer it lawfully. We ask that PCLOB work to cause the declassification of more facts about this unlawful activity, to reach its own assessment as to whether the cause of the problem was remedied, and to report that assessment publicly.

Finally, PCLOB played an important role in the debate around Section 215 by debunking government claims about the effectiveness of bulk collection as an anti-terrorism tool. After extensive investigation, as well as assessing the 54 cases in which the IC claimed that Section 215 or Section 702 "contributed to a success story", the PCLOB determined:

> Based on the information provided to the Board, we have not identified a single instance involving a threat to the United States in which the telephone records program made a concrete difference in the outcome of a counterterrorism investigation. Moreover, we are 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.[16]

This conclusion was crucial to Congress' assessment of the bulk collection program and its decision to end it. We urge you to examine any efficacy claims made by government officials about Section 215 surveillance in the revamped, targeted program with an eye toward debunking efficacy claims that need to be debunked, and confirming efficacy claims that your investigation reveals should be confirmed. Such information will be important to Congress' reassessment of the program later this year.

PCLOB and IC Use of Private Sector Data for Counterterrorism

Increasingly, companies in the United States and abroad are collecting personally identifiable information in order to offer services to users and to customers. Sometimes, the information is collected to train an algorithm for purposes of artificial intelligence or machine learning. Sometimes it is collected for "big data" analytics – to draw intelligence from a huge collection of data that could not be drawn from smaller collections. We expect this collection of personal information to grow as more uses for it are identified.

It makes sense for elements of the intelligence community to seek access to this data for intelligence purposes, and it seems probable that at least some companies would sell this data to intelligence agencies. We are particularly concerned with the possible disclosure by data brokers to governmental entities of metadata which, if sought by the government directly from a communications service provider, could not be disclosed to governmental entities without legal process. We are also concerned with the richness of the data that could be disclosed by brokers because particularly revealing disclosures could, under

[16] 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, January 23, 2014. https://www.pclob.gov/library/215-Report_on_the_Telephone_Records_Program.pdf, p. 146.

Supreme Court precedent, require a warrant (or FISA court order) as we describe below. These concerns are particularly acute with respect to data that concerns U.S. persons.

While some information about the practice of data broker disclosure to governmental entities has emerged in the context of law enforcement, precious little information about intelligence use of such private sector information has been made public. For example, the New York Times reported in May that mobile providers were selling information about the location of mobile phone subscribers to the data broker Securus Technologies, which in turn sold the data to law enforcement and prison officials for the purpose of finding individuals.[17] As a direct result of these disclosures, mobile providers cut their contracts with aggregators of location information, and either pledged to refrain from selling this information altogether, or to limit sales to certain purposes such as roadside assistance.[18] Was, and is, this data also being sold to the IC for counterterrorism and other intelligence purposes?

As another example, one of the largest DNA testing services, Family Tree DNA, recently changed its terms of service to allow the FBI to access DNA submitted by people trying to trace their genealogy. It decided to allow law enforcement the same level of access to its data that members of the public enjoy.[19] This has implications for the privacy of both the person who submitted the data and for their family members. Is DNA data also being made available to the IC for counterterrorism and other intelligence purposes?

We are particularly concerned with law enforcement access to large data sets that would reveal very personal characteristics or activities of persons identifiable through that data, or through that data when co-mingled with other data. The Supreme Court, using very broad language in a fairly narrow case, recently hinted that such collections of data may be available only when law enforcement has a warrant.[20] With respect to cell site location information that was at issue in *Carpenter v. U.S.*, the Court said it "provides an intimate window into a person's life, revealing not only his particular movements, but through them his 'familial, political, professional, religious and sexual associations.'" (citing Justice Sotomayor's concurring opinion in a 2012 GPS tracking case, *U.S. v. Jones*). The *Carpenter* majority said further, "As technology has enhanced the Government's capacity to encroach upon areas normally guarded from inquisitive eyes, this Court has sought to 'assure [] preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted.'" [citing *Kyllo v United States*, a 2001 case establishing that law enforcement officers could not use heat-sensing equipment to draw inferences about what

[17] The New York Times, *Service Meant to Monitor Inmates Calls Could Track You, Too,* May 18, 2018, https://www.nytimes.com/2018/05/10/technology/cellphone-tracking-law-enforcement.html.
[18] The Verge, *Verizon Will Stop Selling Real Time Location Data to Third-Party Brokers,* June 19, 2018. https://www.theverge.com/2018/6/19/17478934/verizon-selling-real-time-location-data-third-party-securus-wyden.
[19] Engaget, *At-home DNA testing company gives the FBI access to its database,* Feb. 1, 2019.
[20] *Carpenter v. United States* (U.S. 2018). https://www.supremecourt.gov/opinions/17pdf/16-402_h315.pdf. The *Carpenter* court took pains to point out that it was not deciding about government access to data for intelligence purposes, but the reasoning the court used could have a spill-over effect in the intelligence context.

is happening inside a home unless they first obtained a warrant.] To what extent are intelligence officials accessing data held by the private sector that would trigger the *Carpenter* warrant requirement? The public does not know.

We urge PCLOB to issue a public report on IC use of private sector data for counterterrorism purposes. It should examine scope and efficacy of such access, the adequacy of the privacy protections surrounding such data, and whether some of the data may be being accessed without compliance with constitutional restrictions. To our knowledge, this would be a new and forward-looking area of inquiry for PCLOB.

PCLOB and Domestic Surveillance To Protect Against Terrorism

The FBI and certain other elements of the IC are responsible for preventing and stopping attacks stemming from both international and domestic terrorism. PCLOB's mandate to "analyze and review actions the executive branch takes to protect the Nation from terrorism" is not confined to international terrorism, and the scope of its review should extend to domestic surveillance to protect against terrorism as well.

In attempting to protect the nation from domestic terrorism, there is a risk that elements of the IC may conflate dissent with violence and subsequently monitor peaceful activity. Such surveillance chills the exercise of First Amendment rights and is a misallocation of resources. It is precisely this type of overreach which concerned civil liberties advocates after 9/11 and that PCLOB was created to monitor.

Unfortunately, federal agencies have inappropriately targeted First Amendment activity, or stretched the definition of a terrorism investigation in order to investigate certain groups.[21] Recently, the FBI identified the Black Lives Matters movement as a surveillance target.[22] A leaked FBI Intelligence Assessment identified "black identity extremists" as a terrorist threat to law enforcement. It raises concerns that the designation will be used to enhance government scrutiny of Black activists.[23] Federal agencies also supported the surveillance

---

[21] For example, a 2010 Department of Justice, Office of Inspector General report reviewing FBI investigations of domestic advocacy organizations from January 2001 to December 2006 found that the FBI investigations of Greenpeace and the Catholic Worker movement treated possible vandalism cases as domestic terrorism cases. The report also found that the FBI improperly collected and retained information about activists' First Amendment activities. https://oig.justice.gov/special/s1009r.pdf. In the early 2000s, the Department of Defense inappropriately included information on anti-war protests in it's TALON database. https://www.aclu.org/report/no-real-threat-pentagons-secret-database-peaceful-protest. DHS's Suspicious Activity Reports are known to encompass innocent First Amendment activity like photography, which DHS continues to highlight as suspicious. https://www.cjr.org/united_states_project/homeland-security-photography-warning.php.

[22] The Intercept, *FBI Tracked an Activist Involved With Black Lives Matter As They Travelled Across the U.S., Documents Show,* March 19, 2018. https://theintercept.com/2018/03/19/black-lives-matter-fbi-surveillance/

[23] Foreign Policy, *The FBI's New U.S. Terrorist Threat: "Black Identity Extremists,"* October 6, 2017. https://foreignpolicy.com/2017/10/06/the-fbi-has-identified-a-new-domestic-terrorist-threat-and-its-black-identity-extremists/.

of protesters of the North Dakota Access Pipeline and Keystone XL pipeline.[24] Furthermore records show that the FBI maintained records on peaceful climate change protesters,[25] and opened a domestic terrorism investigation into BAMN, a civil rights group.[26] We urge PCLOB to investigate such surveillance and to issue a public report about it.

In addition to the inappropriate targeting of domestic groups for terrorism and related investigation, the Administration recently stood up a new National Vetting Center (NVC) designed to facilitate information sharing "to identify potential threats to national security, border security, homeland security, and public safety."[27] We are concerned about the types and reliability of the data that will be shared at the NVC. In particular, we are concerned that social media data, which the State Department has taken steps to collect as a part of visa applications, will be shared.[28] Social media information is unlikely to yield relevant security information because it is of such limited utility in predicting violent conduct.[29] Social media content is not easily interpreted and reliance on it – because of the volume involved – will likely lead to the use of problematic algorithmic screening. Social media surveillance will chill the free speech and association of Americans and non-citizens. PCLOB should review this collection program and the NVC's sharing of social media information, and assess the utility of social media monitoring in combating terrorism as well as the impact of such monitoring on free expression rights of immigrants and Americans.

Conclusion

Thank you again for the opportunity to testify at today's public forum. As I said at the outset, we recognize that PCLOB was only recently reconstituted with a quorum and that it has limited resources. We hope, however, that some of those resources can be devoted to completing and seeking declassification of E.O. 12333 reports, re-examining Section 215 of the USA PATRIOT Act, issuing a report on IC use of private sector data, and investigating

---

[24] The Guardian, *Keystone protesters tracked at border after FBI spied on 'extremists,'* June 8, 2015. https://www.theguardian.com/us-news/2015/jun/08/keystone-protesters-fbi-watchlisted-terrorism; The Guardian, *Revealed: FBI violated its own rules while spying on Keystone XL opponents,* May 12, 2018. https://www.theguardian.com/us-news/2015/may/12/revealed-fbi-spied-keystone-xl-opponents.

[25] The Guardian, *Revealed: FBI kept files on peaceful climate change protesters,* Dec. 13, 2018. https://www.theguardian.com/us-news/2018/dec/13/fbi-climate-change-protesters-iowa-files-monitoring-surveillance-.

[26] The Guardian, *Revealed: FBI Investigated civil rights group as 'terrorism' threat and viewed KKK as victims,* Feb. 1, 2019. https://www.theguardian.com/us-news/2019/feb/01/sacramento-rally-fbi-kkk-domestic-terrorism-california.

[27] Department of Homeland Security, *The National Vetting Center,* February 6, 2018. https://www.dhs.gov/news/2018/02/06/national-vetting-center.

[28] Center for Democracy & Technology, *The Office of Management and Budget Should deny the State Department's Proposal to Collect Social Media Identifiers from 14.7 Million Visa Applicants,* September 28, 2018. https://cdt.org/blog/the-office-of-management-and-budget-should-deny-the-state-departments-proposal-to-collect-social-media-identifiers-from-14-7-million-visa-applicants/.

[29] *See* 2018 CDT report on Digital Decisions, https://cdt.org/issue/privacy-data/digital-decisions/.

domestic surveillance of protest and other vulnerable groups, particularly the use of social media information in such surveillance.