PROJECT ON GOVERNMENT OVERSIGHT

Thank you for the opportunity to submit testimony to the Privacy and Civil Liberties Oversight Board (PCLOB) on various issues surrounding surveillance pursuant to the Foreign Intelligence Surveillance Act (FISA) and other relevant issues.

I am Jake Laperruque, senior counsel for The Constitution Project at the Project On Government Oversight (POGO). POGO is a nonpartisan independent watchdog that investigates and exposes waste, corruption, abuse of power, and when the government fails to serve the public or silences those who report wrongdoing. We champion reforms to achieve a more effective, ethical, and accountable federal government that safeguards constitutional principles. The Constitution Project at POGO strives to protect individuals from improper and overbroad surveillance, especially when such surveillance is conducted in the name of national security.

The Constitution Project has long advocated for increased accountability, oversight, and proper checks of a FISA process that is too often subject to scrutiny that is too weak.[1]

My testimony examines a variety of legal and policy issues across a wide array of surveillance authorities; before discussing each of these issues in turn, I believe it is valuable to note several key observations relating to national security surveillance that affect virtually all of the issues FISA addresses.

First, over the past several decades, FISA surveillance has significantly shifted in focus from counterespionage to counterterrorism. This has inherently pulled FISA into the realm of law enforcement investigations and activities. Yet, even as FISA has increasingly become a tool for domestic law enforcement, there has not been a similar shift in safeguards on these authorities to ensure the protection of due process and civil liberties that is expected of criminal proceedings. Rather, the rules and accountability structures still largely treat FISA surveillance as an authority more focused on foreign affairs.

Second, we know extremely little about the impact FISA surveillance has on individuals. It is important that surveillance not only be seen as harmful when it leads to abuse or improper public disclosure of private information; the collection of sensitive information by the government is in itself a harm to privacy, regardless of how that information is used. A key principle our constitutional system is founded upon is that any invasion of privacy must be reasonable in light of that harm.

[1] The Constitution Project's Liberty and Security Committee, *The Case for a FISA "Special Advocate"* (May 29, 2014). https://archive.constitutionproject.org/wp-content/uploads/2014/05/The-Case-for-a-FISA-Special-Advocate_FINAL.pdf

Therefore, in examining the impact of FISA surveillance it is essential not only to know how FISA surveillance might be abused, subject to compliance problems, or used in investigations—although in these areas there are serious problems with proper transparency as well—but also to know the full scale of who is subject to surveillance. This requires improved transparency about how certain aspects of FISA are used in general, as well as a new focus on assessing whether FISA is having a disparate impact on specific communities and demographic populations.

Third, there is still far too little transparency and far too much secrecy regarding FISA and intelligence community surveillance activities; in a democratic society, it is essential that the populace has access to how the government interprets the law and wields its power.

In recent years the intelligence community has taken some positive steps toward increasing transparency, such as the significant declassifications prompted by PCLOB's reports on the telephony bulk collection program and Section 702 of FISA. Increased intelligence community transparency occurred in response to the explosive disclosures made by Edward Snowden and the public outcry and condemnation of surveillance activities by Congress and courts that followed, a motivation that has waned even as the need for increased public awareness remains.[2]

The limited reforms to increase transparency have been insufficient to answer critical questions concerning how much and in what ways FISA surveillance impacts individuals. And in some areas, we have seen a troubling backslide toward improper secrecy. For example, the Office of the Director of National Intelligence (ODNI) reneged on an explicit commitment to Congress to provide an estimate of the number of U.S. persons affected by Section 702 surveillance[3]; this decision left both Congress and the public in the dark during the most recent reauthorization debate of that surveillance authority as to how many individuals Section 702 impacted. The intelligence community also delayed the release of a significant FISA Court opinion that was highly critical of government surveillance practices for almost a full year absent any justification or apparent need.[4] This was a clear breach of the requirements Congress had established in the USA FREEDOM Act of 2015 for prompt declassification of significant opinions, a breach that led both the House and Senate earlier this year to pass stricter disclosure requirements to prevent a recurrence of this failure.[5] And

[2] Jack Goldsmith, "Three Years Later: How Snowden Helped the U.S. Intelligence Community," *Lawfare*, June 6, 2016. https://www.lawfareblog.com/three-years-later-how-snowden-helped-us-intelligence-community

[3] Dustin Volz, "NSA backtracks on sharing number of Americans caught in warrant-less spying," Reuters, June 9, 2017. https://www.reuters.com/article/us-usa-intelligence/nsa-backtracks-on-sharing-number-of-americans-caughtin-warrant-less-spying-idUSKBN19031B

[4] Elizabeth Goitein, "How the FBI Violated the Privacy Rights of Tens of Thousands of Americans," The Brennan Center for Justice, October 22, 2019. https://www.brennancenter.org/our-work/analysis-opinion/how-fbi-violated-privacy-rights-tens-thousands-americans ("... the government sat on the FISA Court's October 2018 opinion for almost a year, instead of promptly declassifying and releasing it as envisioned by Congress in the 2015 USA FREEDOM Act.")

[5] Although the legislative history of the 2015 USA FREEDOM Act debate makes clear that Congress viewed the law as requiring prompt disclosure of significant opinions, the recent delay led both the House and Senate to pass versions of the USA FREEDOM Reauthorization Act of 2020, H.R.6172, with an identical provision placing a strict 180-day requirement for disclosure.

during the recent debate regarding Section 215, the National Security Agency (NSA) repeatedly claimed the now defunct call detail records program had value while refusing to answer the most basic questions as to whether it had contributed to the discovery or disruption of any national security threats.[6]

PCLOB can and should work to address these issues across many different areas of how FISA operates. Below are a key set of issues we believe PCLOB should prioritize, including recommended transparency goals the board should undertake and policy proposals it should advocate that Congress enact into law.

Increase public understanding of how FISA surveillance impacts individuals

The scale of FISA surveillance and the number of people whose privacy is harmed by it is massive, yet the public still has far too little knowledge about it. PCLOB should prioritize changing this, and providing increased transparency and public understanding on how FISA surveillance impacts individuals.

Lack of information on how many U.S. persons are harmed by warrantless FISA surveillance

Probably the most significant form of FISA surveillance in terms of how many U.S. persons—and individuals in general—it impacts is the warrantless surveillance system, Section 702. Not only is the scale of Section 702 surveillance enormous, it also has recently increased significantly.

When Congress reauthorized Section 702 in January 2018,[7] the most recently released number of targets was 106,469,[8] for 2016. Since then, that number has nearly doubled to 204,968 for 2019.[9]

---

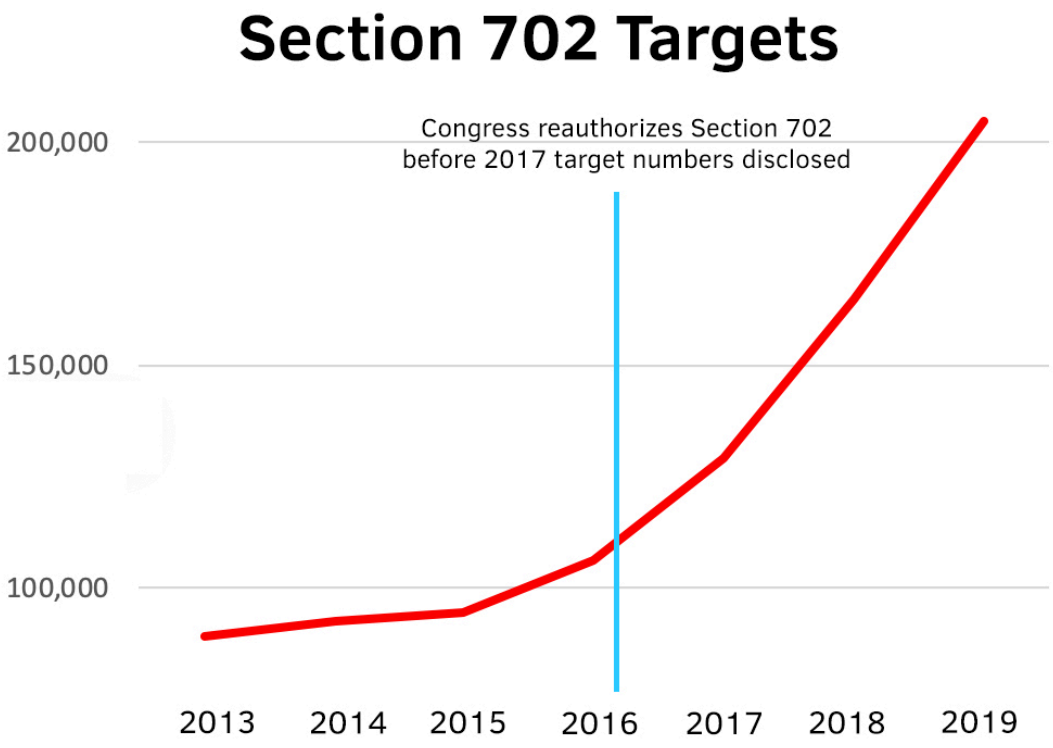
[6] Emily Birnbaum, "Senators press NSA official over shuttered phone surveillance program," *The Hill*, November 6, 2019. https://thehill.com/policy/technology/469268-senators-press-nsa-official-over-shuttered-phone-surveillance-program; *Reauthorizing the USA FREEDOM Act of 2015: Hearing Before the Senate Committee on the Judiciary*, 116th Cong. (November 6, 2019). https://www.judiciary.senate.gov/meetings/reauthorizing-the-usa-freedom-act-of-2015

[7] Robyn Greene, "Americans Wanted More Privacy Protections. Congress Gave Them Fewer," *Slate*, January 26, 2018. https://slate.com/technology/2018/01/congress-reauthorization-of-section-702-of-the-fisa-is-an-expansion-not-a-reform.html

[8] At the time Section 702 was reauthorized, the most recently released data on Section 702 targeting was from April 2017, which disclosed the 2016 calendar year target number of 106,469. Office of the Director of National Intelligence, Office of Civil Liberties, Privacy, and Transparency, *Statistical Transparency Report Regarding Use of National Security Authorities Calendar Year 2016* (April 2017). https://www.dni.gov/files/icotr/ic_transparecy_report_cy2016_5_2_17.pdf

[9] Office of the Director of National Intelligence, Office of Civil Liberties, Privacy, and Transparency, *Statistical Transparency Report Regarding Use of National Security Authorities Calendar Year 2019* (April 2020). https://www.dni.gov/files/CLPT/documents/2020_ASTR_for_CY2019_FINAL.pdf

This most recent target number constituted a 24% increase over the previous year, the continuation of a notable and disturbing shift: In 2014 and 2015, Section 702 targets increased by less than 5% over the prior year; in 2016, targets increased by about 13%; and over the past three years—for which all data on number of targets was released after the reauthorization of Section 702—the number of Section 702 targets has grown by over 20% each year.[10]



(Project On Government Oversight; Source: Office of the Director of National Intelligence, Office of Civil Liberties, Privacy, and Transparency, Statistical Transparency Report Regarding Use of National Security Authorities Calendar Year 2019 (April 2020) [see note 9].)

Put simply: The scale of Section 702 surveillance has dramatically increased in the years since PCLOB last released a full report on this topic.[11] And while PCLOB recommended releasing various forms of information to indicate how often Section 702 surveillance collects the communications of U.S. persons, because of inaction by the intelligence community, the public

[10] Specifically, the 2019 number of targets grew by 40,198, a 24% increase from the prior year; in 2018, the number of targets grew by 35,690, nearly a 28% increase; in 2017, the number of targets grew by 22,611, a 21% increase. In contrast, in 2016, the targets grew by 12,101, a 13% increase; in 2015, the targets grew by 1,661, a 2% increase; in 2014, the targets grew by 3,569, a 4% increase. Office of the Director of National Intelligence, *Statistical Transparency Report Regarding Use of National Security Authorities Calendar Year 2019* [see note 9].

[11] Privacy and Civil Liberties Oversight Board, *Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act* (July 2, 2014). https://documents.pclob.gov/prod/Documents/OversightReport/823399ae-92ea-447a-ab60-0da28b555437/702-Report-2.pdf

knows no more now about how many U.S. persons this warrantless surveillance system affects than it did when PCLOB's report was released in 2014.

The lack of information in this area is a result of shifting commitments and priorities by the intelligence community. Following a direct promise to Congress and similar assurances to civil liberties advocates to provide an estimate of U.S. persons impacted by Section 702 surveillance, ODNI reneged on its commitments in 2017.[12] The ODNI based this abrupt shift on two claims: that it was suddenly infeasible to provide an estimate, and that conducting a count would create risks to privacy. ODNI has never publicly substantiated the first reason, and the second had already been accounted for and discredited by civil liberties advocates even before ODNI made the claim.[13]

It is critical that the public has a basic understanding of how much Section 702's warrantless surveillance system collects their private calls, texts, chats, and emails. POGO recommends that PCLOB:

- *work to ensure that the intelligence community develops and publicly reports, in a timely manner, an estimate of U.S. persons whose communications are collected[14];*
- *advocate for a statutory requirement that the intelligence community provide such a publicly available estimate on an annual basis; and*
- *investigate and publicly report on the veracity of ODNI's claims that new circumstances limited its ability to conduct an estimate of the number of affected U.S. persons, beginning in December 2016 when ODNI committed to Congress to provide an estimate and continuing through June 2017 when ODNI refused to do so.*

Lack of information on what groups FISA surveillance most harms and disparate impact

Beyond lack of knowledge on the scale of impact of Section 702, a significant problem exists regarding transparency of all forms of FISA surveillance in terms of what groups it most impacts.

---

[12] Dustin Volz, "NSA backtracks on sharing number of Americans caught in warrant-less spying," Reuters, June 9, 2017. https://www.reuters.com/article/us-usa-intelligence/nsa-backtracks-on-sharing-number-of-americans-caughtin-warrant-less-spying-idUSKBN19031B; Letter from House Judiciary Members to Director of National Intelligence James Clapper on discussions regarding Section 702 surveillance transparency, December 16, 2016. https://judiciary.house.gov/sites/democrats.judiciary.house.gov/files/documents/letter%20to%20director%20clapper%20(12.16.16).pdf

[13] *Open Hearing on FISA Legislation: Hearing Before the Senate Select Committee on Intelligence*, 115th Cong. (June 7, 2017) https://www.intelligence.senate.gov/hearings/open-hearing-fisa-legislation-0#; Letter from Civil Society Groups to Director of National Intelligence James Clapper on Section 702 surveillance and transparency, October 29, 2015. https://www.brennancenter.org/sites/default/files/analysis/Coalition_Letter_DNI_Clapper_102915.pdf

[14] Civil liberties advocates have already demonstrated a clear consensus that efforts undertaken to acquire such an estimate will have a net positive impact on privacy, and that sampling and necessary qualifiers (such as potentially tabulating individuals in the U.S. in place of U.S. persons) are acceptable components of deriving a best possible estimate. See, for example: Letter from Civil Society Groups to Director of National Intelligence James Clapper [see note 13].

Surveillance conducted in the name of national security has in many cases been directed at racial, ethnic, and religious minorities. In the 1950s, 1960s, and 1970s, the FBI surveilled and targeted civil rights leaders such as Dr. Martin Luther King Jr. through its "Racial Matters Program," as well as through COINTELPRO, or Counterintelligence Program.[15] From the 1990s through the early 2010s, the Drug Enforcement Administration engaged in bulk collection of records of Americans' international phone calls[16]—a precursor to the Section 215 telephony bulk collection program—and targeted calls to and from countries including most of Latin America, meaning the program likely had a disproportionate impact on immigrants, and Latino immigrants in particular.[17] In the 2000s and 2010s, the New York City Police Department operated a surveillance unit focused on monitoring Muslim communities, with assistance from the CIA.[18] At the same time, FBI trainings instructed investigators to target Muslims based on their religion, claiming that being a devout Muslim made individuals more likely to be violent and to sympathize with terrorists.[19] In recent years, the FBI has created a "Black Identity Extremist" label to direct surveillance at Black activists engaged in First Amendment-protected activism and protests.[20] And as recently as June 2020, senior leadership at the FBI called for the bureau to direct intense surveillance, including use of "robust social media exploitation teams," at demonstrators advocating for the civil rights of Black Americans, comparing the protests to the September 11 attacks.[21]

Improper targeting and surveillance that disproportionately impacts certain groups inflicts a variety of harms. It directly undercuts equal protection as guaranteed by the Fourteenth Amendment, and it perpetuates racial injustice, inequality, and discrimination.

---

[15] The Martin Luther King, Jr. Research and Education Institute, "Federal Bureau of Investigation (FBI)." https://kinginstitute.stanford.edu/encyclopedia/federal-bureau-investigation-fbi (Downloaded April 3, 2019). See also Jeffrey O.G. Ogbar, "The FBI's War on Civil Rights Leaders," *The Daily Beast*, January 16, 2017. https://www.thedailybeast.com/the-fbis-war-on-civil-rights-leaders

[16] Office of the Inspector General, U.S. Department of Justice, *A Review of the Drug Enforcement Administration's Use of Administrative Subpoenas to Collect or Exploit Bulk Data* (March 2019), 15-18. https://oig.justice.gov/reports/2019/o1901.pdf

[17] Brad Heath, "U.S. secretly tracked billions of calls for decades," *USA Today*, April 8, 2015. https://www.usatoday.com/story/news/2015/04/07/dea-bulk-telephone-surveillance-operation/70808616/; Alvaro M. Bedoya, "The Color of Surveillance: What an infamous abuse of power teaches us about the modern spy era," *Slate*, January 18, 2016. https://slate.com/technology/2016/01/what-the-fbis-surveillance-of-martin-luther-king-says-about-modern-spying.html ("The NSA's call records program—the single largest domestic spying program in our nation's history—was effectively beta-tested for almost a decade on American immigrants. Countless immigrants' calls were tracked by the DEA when they called home. This is particularly true for Hispanic immigrants, who make up a large part of what is now the largest minority group in the country.")

[18] American Civil Liberties Union, "Factsheet: The NYPD Muslim Surveillance Program." https://www.aclu.org/other/factsheet-nypd-muslim-surveillance-program (accessed July 20, 2020); Adam Goldman and Matt Apuzzo, "With cameras, informants, NYPD eyed mosques," Associated Press, February 23, 2012. https://www.ap.org/ap-in-the-news/2012/with-cameras-informants-nypd-eyed-mosques; Matt Apuzzo and Joseph Goldstein, "New York Drops Unit That Spied on Muslims," *New York Times*, April 15, 2014. https://www.nytimes.com/2014/04/16/nyregion/police-unit-that-spied-on-muslims-is-disbanded.html; Faiza Patel, "What Is the CIA Teaching the NYPD?" The Brennan Center, August 15, 2013. https://www.brennancenter.org/our-work/research-reports/what-cia-teaching-nypd

[19] Spencer Ackerman, "FBI Teaches Agents: 'Mainstream' Muslims Are 'Violent, Radical,'" *Wired*, September 14, 2011. https://www.wired.com/2011/09/fbi-muslims-radical/

[20] American Civil Liberties Union, "Leaked FBI Documents Raise Concerns about Targeting Black People Under 'Black Identity Extremists' and Newer Labels," Press Release, August 9, 2019. https://www.aclu.org/press-releases/leaked-fbi-documents-raise-concerns-about-targeting-black-people-under-black-identi-1

[21] Zolan Kanno-Youngs et al., "From the Start, Federal Agents Demanded a Role in Suppressing Anti-Racism Protests," *New York Times*, July 28, 2020. https://www.nytimes.com/2020/07/28/us/federal-agents-portland-seattle-protests.html

Unfortunately, surveillance ostensibly conducted for national security purposes that improperly targets or disproportionately impacts marginalized communities generally only comes to light long after it has occurred. And we have no notion of how much various FISA surveillance authorities—including targeted FISA warrants, collection authorities such as Section 215 and National Security Letters, and warrantless Section 702 surveillance—impact different groups, whether certain affiliations such as religion or participation in civil rights organizations play a role in targeting, or if there are patterns of disparate impact in who is surveilled.

Shedding light on these important issues should be a priority for the board moving forward. POGO recommends that PCLOB:

- *examine and publicly report on to what extent First Amendment-protected categories and activities—such as religious affiliation and protesting—are used as a basis for designating individuals as a target for various forms of FISA surveillance;*
- *examine and publicly report on the extent to which racial, ethnic, and religious groups are disproportionately targeted pursuant to various forms of FISA surveillance; and*
- *examine and publicly report on the extent to which racial, ethnic, and religious groups are disproportionately impacted by forms of FISA surveillance.*

Address danger of using FISA surveillance to derive evidence and failing to disclose how evidence was discovered

Another significant problem with FISA is the lack of disclosure of how it is used to develop and derive evidence.[22] This hampers public knowledge and transparency, and undermines the constitutional rights of individuals who have the right to know—and challenge—the use of FISA as a component of a criminal investigation and prosecution.

Disclosing not only the methods used to directly obtain evidence but also the methods and techniques—such as FISA surveillance—that were originally used to *derive* evidence is critical to protecting constitutional rights. Refusing to disclose how evidence was derived leaves individuals vulnerable to overbroad surveillance that violates Fourth Amendment rights and statutory limits. It also destroys a key safeguard against willful abuse that the exclusionary rule was designed to prevent: The notion that improper collection of evidence will not aid investigations, because violations of Fourth Amendment rights and statutory limits will come to light during court proceedings and that improperly acquired evidence would then be dismissed.

[22] Patrick C. Toomey, "Government Engages In Shell Game To Avoid Review Of Warrantless Wiretapping," American Civil Liberties Union, June 25, 2013. https://www.aclu.org/blog/national-security/secrecy/government-engages-shell-game-avoid-review-warrantless-wiretapping; Patrick C. Toomey, "Why Aren't Criminal Defendants Getting Notice of Section 702 Surveillance — Again?" *Just Security*, December 11, 2015. https://www.justsecurity.org/28256/arent-criminal-defendants-notice-section-702-surveillance-again/

The risks are all the more severe if the government not only fails to disclose surveillance methods evidence was derived from but also uses "parallel construction"—manufacturing a second, alternate source of how evidence was derived—to obfuscate the source and prevent due inquiry.

Unfortunately, right now the intelligence community is effectively its own watchdog, responsible for preventing—or permitting—the government from improperly cloaking use of FISA surveillance to obtain evidence. This is because the executive branch sets its own definition of what "derive" means, allowing the government to hide use of FISA surveillance by creating a narrow definition to argue that evidence is almost never "derived" from FISA. The public has no knowledge of how the Department of Justice interprets "derive" in the context of FISA surveillance, despite longstanding concerns from privacy advocates that the term is being misappropriated to hide the role of FISA surveillance in investigations.[23] Parallel construction is a method of blocking defendants from seeing how evidence was derived and preventing them and courts from realizing that the government is hiding its original source.[24]

These problems are amplified by the fact that FISA surveillance provides the government unusually easy access to sensitive materials and private information. Section 215 and National Security Letter authorities can lead to seizure of individuals' private records absent any suspicion of wrongdoing, merely because those records were relevant to an investigation. And warrantless queries of U.S. persons' communications obtained via Section 702—also known as the "backdoor search loophole"—similarly provides access to private communications absent suspicion. The government has used this authority to conduct bulk-style generalized queries to seek out the communications of large numbers of individuals without a warrant in one fell swoop.[25] The backdoor search loophole is in itself a violation of privacy rights, and by removing courts from examination of Americans' communications also facilitates undisclosed use of FISA for prosecutions.

The ease that FISA allows for acquisition of private information and communications increases the likelihood that it could be used to derive evidence in investigations, and it heightens the potential for deprivation of constitutional rights that defendants should be entitled to challenge.

---

[23] Ashley Gorski, "Shouldn't You Be Able To See the Secret Surveillance Orders That Could Put You in Prison?" American Civil Liberties Union, February 19, 2015. https://www.aclu.org/blog/speakeasy/shouldnt-you-be-able-see-secret-surveillance-orders-could-put-you-prison; Toomey, "Why Aren't Criminal Defendants Getting Notice of Section 702 Surveillance — Again?" [see note 22]; *Reauthorizing the USA FREEDOM Act of 2015: Hearing Before the Senate Committee on the Judiciary*, 116th Cong. (November 6, 2019) (testimony of Elizabeth Goitein, Co-Director of the Liberty and National Security Program, The Brennan Center). https://www.judiciary.senate.gov/imo/media/doc/Goitein%20Testimony.pdf

[24] Human Rights Watch, *Dark Side: Secret Origins of Evidence in US Criminal Cases* (January 2018). https://www.hrw.org/sites/default/files/report_pdf/us0118.pdf

[25] [REDACTED], No. [REDACTED], 68 (FISA Ct. Oct. 18, 2018) (unpublished). https://www.intel.gov/assets/documents/702%20Documents/declassified/2018_Cert_FISC_Opin_18Oct18.pdf; Dustin Volz and Byron Tau, "FBI's Use of Surveillance Database Violated Americans' Privacy Rights, Court Found," *Wall Street Journal*, October 8, 2019. https://www.wsj.com/articles/fbis-use-of-foreign-surveillance-tool-violated-americans-privacy-rights-court-found-11570559882

It is vital that the public understand how the government can use FISA in criminal investigations, and that defendants are able to exercise their right to review and challenge government surveillance that was used to derive evidence against them. POGO recommends that PCLOB:

- *examine, publicly report on, and work to ensure declassification of all government interpretations of what constitutes "derivative evidence" in relation to FISA;*
- *advocate for statutory requirements that will ensure defendants receive notice whenever FISA is used to derive evidence, and prohibit use of parallel construction to obstruct defendants' access to relevant information in the case against them;*
- *advocate for improved auditing procedures to ensure compliance with the needed notice requirements and recommended prohibition of parallel construction; and*
- *advocate for statutory requirements that will close the "backdoor search loophole" and end warrantless U.S. person queries of Section 702 information.*

Respond to unclear and overbroad FISA authorities to collect "business records" and records in possession of a third party

Despite significant scrutiny and reforms over the past decade, serious questions and problems remain about FISA surveillance authorities that facilitate the collection of business records, which could include phone, internet, travel, and other records of any person in the possession of a business.[26] PCLOB should work to provide clarity and increase public knowledge on this central issue, while also promoting policy reforms to constrain unnecessarily broad authorities.

Section 215

While much focus on Section 215 in recent years has centered on its use for collecting phone records on a mass scale, this authority also allows the collection of a huge array of private records that can reveal sensitive information. There is an urgent need to understand what types of records the government uses Section 215 to collect and how often various categories of records are obtained, given the potential for such records to reveal sensitive political, professional, medical, religious, and sexual associations and activities.

Two recent events increase the urgency of facilitating public knowledge regarding what types of records Section 215 is used to collect. First, the Supreme Court's 2018 decision in Carpenter v. United States significantly upended the third-party doctrine, which the government had relied on to argue that its use of Section 215 to collect records held by a third party did not impact Fourth Amendment rights.[27] The court explicitly stated that for records such as cellphone location data, which are near-universally maintained by third

[26] Jake Laperruque, "The History and Future of Mass Metadata Surveillance," Project On Government Oversight, June 11, 2019. https://www.pogo.org/analysis/2019/06/the-history-and-future-of-mass-metadata-surveillance/

[27] Carpenter v. United States, 138 S. Ct. 2206 (2018). https://www.supremecourt.gov/opinions/17pdf/16-402_h315.pdf

parties and can reveal sensitive information, "the fact that the information is held by a third party does not by itself overcome the user's claim to Fourth Amendment protection."[28] This enhanced standard of protection for privacy makes it critical that the public know what types of records the government obtains with Section 215 to ensure that the government comports with the letter and spirit of Carpenter.

Second, Congress has recently undertaken efforts to enact legislative limits that prohibit the use of Section 215 to collect certain types of data.[29] Improved knowledge of what categories of information Section 215 is used to collect and how often it is used will aid Congress's ability to develop appropriate and effective laws.

The public deserves far more information about how the government uses Section 215 to obtain their private information and about what authority the government relies on in doing so. POGO recommends that PCLOB:

- *examine, report on, and work to ensure declassification of the government's interpretation of the Carpenter decision and its effect on FISA surveillance, especially in relation to the collection of third-party records;*
- *examine and report on what categories of records and information Section 215 is used to collect, and the potential privacy harms emanating from such collection; and*
- *advocate for statutory requirements that prevent the use of Section 215 to collect location data and movements, web browsing activity, medical records, and other highly sensitive data.*

National Security Letters

National Security Letter authorities—a set of statutes that allow the government to directly demand business records without any judicial authorization—permit the same harms from the collection of sensitive records as Section 215, but are not subject to independent oversight from the courts. Given the government's history of compliance problems and misconduct regarding FISA surveillance,[30] as well as use of FISA business records authorities to make overbroad demands for records that courts found improper,[31] the absence of independent oversight of judges for collection through use of National Security Letters is deeply problematic.

---

[28] Carpenter v. United States, 11 [see note 27].

[29] See USA FREEDOM Reauthorization Act of 2020, H.R. 6172, 116th Cong. (2020). https://www.congress.gov/bill/116th-congress/house-bill/6172/text

[30] Demand Progress, "Institutional Lack of Candor" (September 21, 2017). https://s3.amazonaws.com/demandprogress/reports/FISA_Violations.pdf; Demand Progress and FreedomWorks, *Section 215: A Brief History of Violations* (September 2019) https://s3.amazonaws.com/demandprogress/reports/sec-215-violations-report.pdf; Office of the Inspector General, U.S. Department of Justice, *Review of Four FISA Applications and Other Aspects of the FBI's Crossfire Hurricane Investigation* (December 2019). https://www.justice.gov/storage/120919-examination.pdf

[31] *ACLU v. Clapper*, No. 14-42 (2d *Cir.*, 2015). https://www.justsecurity.org/wp-content/uploads/2015/05/14-42.majority.pdf

By all indications, the lax rules for National Security Letters are unnecessary as well as dangerous. Section 215 provides ample capability to obtain the same type of records that National Security Letters are used for, and at the same low standard of relevance to an investigation. Furthermore, if exigent circumstances made taking the time to appear before a judge a genuine danger—rather than just an inconvenience—the emergency authority granted in Section 215 provides the ability to seek records immediately and go before a court to justify that action afterwards.

There may be a select set of categories of data—such as basic subscriber information—where the privacy risks are sufficiently minimal to weigh the inconvenience of investigators needing to make a request before a court as a factor. It would be valuable for PCLOB to evaluate what, if any, records meet this low threshold of privacy danger. But for the vast majority of business records, the harm to privacy clearly warrants independent oversight and judicial scrutiny.

National Security Letters are an overbroad and seemingly unnecessary authority that is ripe for abuse. POGO recommends that PCLOB:

- *examine and report on what categories of records and information National Security Letters are used to collect, and the risk of privacy harms that is created by collecting each type of record;*
- *examine and report on whether National Security Letters provide any novel value that cannot be obtained through the use of Section 215; and*
- *advocate for statutory reforms that either remove National Security Letter authorities or restrict them to highly limited categories such as basic subscriber information.*

Act on the growing risk of content-based collection

Content-based collection—meaning surveillance activities in which automated tools are used to scan content—is also a serious threat to privacy because the government uses that automated analysis to justify searches and seizures. The concept of content-based collection is anathema to the principles the Fourth Amendment is built on, that searches and seizures are based on previously established, reasonable levels of suspicion. Yet in recent years the government, in its FISA surveillance activities, has been embracing content-based collection as a tool.

We have seen several important examples of this in recent years. Most notable, "about" collection of communications that mention a target but are neither to nor from that target is a controversial practice the government asserts the authority to conduct under Section 702.[32] PCLOB previously recommended that the NSA work to seek out technical solutions to limit collection of "about" communications.[33] While "about" collection is currently prohibited by the

[32] Privacy and Civil Liberties Oversight Board, *Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act*, 7 [see note 11].
[33] Privacy and Civil Liberties Oversight Board, *Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act*, Recommendation 7, 144-145 [see note 11].

FISA Court, this restriction is based on technical problems with the practice rather than on legal or constitutional objections[34]; this controversial practice could potentially be resumed in the future. Additionally, in 2016 either the NSA or the FBI sent an order to Yahoo to conduct a scan of emails and return communications based on content within those emails.[35] It is unclear if this was a rare instance or part of a recurring practice.

As automated scanning technologies become more readily available, we will increasingly be forced to encounter the dangers content-based collection could pose as a surveillance practice. We have already seen how the ability for intelligence agencies to scan written text can dramatically increase the scale of collection absent suspicion of wrongdoing. The government could soon come to use automated scanning tools for imagery, such as face and object recognition, to conduct content-based collection—if it isn't doing so already. It could seek to scan images that individuals have sent in texts and emails, or have stored in the cloud. For example, while the NSA currently uses email addresses and phone numbers belonging to targets as selectors for Section 702 collection, it could seek to use face prints (the identifying features for a facial recognition match) of targets as a selector to justify Section 702 collection.

Content-based collection is a serious risk not only because it turns on its head the basic concept that searches and seizures should be predicated on due suspicion, but also because automated scanning tools are prone to significant error. We have already seen this in "about" collection, which was prone to significant overcollection even by the weak standards it operated under.[36] The accuracy of facial recognition can vary significantly based on a variety of factors; it is also more likely to misidentify individuals with darker skin.[37] The reliability of automated scanning technology and artificial intelligence should be subjected to significant scrutiny, and such scrutiny cannot occur if automated scanning is occurring as part of FISA surveillance, which is often exempt from public awareness or debate.

Content-based collection is a highly problematic practice that should not occur in general, and especially not under the cloak of secrecy FISA can provide for untested surveillance methods. POGO recommends that PCLOB:

- *advocate for statutory reforms to fully prohibit "about" collection;*
- *examine and report on whether there have been other instances of collection centered on the content of communications akin to the intelligence community's demand that Yahoo scan its email databases and turn over certain communications based upon their content; and*

[34] Charlie Savage, "N.S.A. Halts Collection of Americans' Emails About Foreign Targets," *New York Times*, April 28, 2017. https://www.nytimes.com/2017/04/28/us/politics/nsa-surveillance-terrorism-privacy.html

[35] Joseph Menn, "Exclusive: Yahoo secretly scanned customer emails for U.S. intelligence – sources," Reuters, October 4, 2016. https://www.reuters.com/article/us-yahoo-nsa-exclusive-idUSKCN1241YT

[36] Savage, "N.S.A. Halts Collection of Americans' Emails About Foreign Targets" [see note 34].

[37] Task Force on Facial Recognition Surveillance, Project On Government Oversight, *Facing the Future of Surveillance* (March 4, 2019). https://www.pogo.org/report/2019/03/facing-the-future-of-surveillance/

- *examine and report on whether the content of images, such as face prints, are used as Section 702 selectors, and whether facial recognition or other types of automated image scanning technologies are used in any component of FISA to justify any form of content-based collection.*

Expand the role of the FISA Court amici

The amicus curiae role for novel and significant questions before the FISA Court created as part of the USA FREEDOM Act has improved the FISA process in notable ways. Amici have been brought into at least 11 cases to provide added perspective to the FISA Court, resulting in substantial deliberations over important issues such as the constitutionality of warrantless U.S. person queries of Section 702 databases.[38] Additionally, the one significant concern raised during the debate over creation of the amicus role—that it might slow or impede FISA Court proceedings[39]—has not been borne out over the five years the amici role has existed; there are no known instances when the amicus's involvement in any way hampered FISA Court proceedings.

The amicus role is unnecessarily limited in several important ways that impair the amici's ability to effectively aid the court and improve the FISA process. First, the set of deliberations the amici are permitted to participate in is too limited. In addition to the current involvement of amici in novel and significant questions of law, their outside voices should also be brought in to participate in deliberations that impact First Amendment-protected activities, as well as those deliberations that raise other serious concerns about civil rights and civil liberties. The amici could also be permitted to review or participate in applications for FISA Title I warrants to monitor U.S. persons. In these cases, the amici would not act as adversarial counsel representing the target, but rather act to prevent the type of misrepresentations or improprieties shown by a December 2019 Department of Justice inspector general report to have occurred.[40]

The amici should also have the ability to directly request that the FISA Court of Review take up a case. It is nonsensical that, if the FISA Court sides with the amicus, the Justice Department can appeal, but if the FISA Court rules in favor of the Justice Department, the amicus cannot appeal.[41]

Additionally, the amici are limited in their resources and access to materials.[42] In order to effectively perform their role, the amici should have access to all FISA Court documents and

---

[38] Faiza Patel and Raya Koreh, "Improve FISA on Civil Liberties by Strengthening Amici," *Just Security*, February 26, 2020. https://www.justsecurity.org/68825/improve-fisa-on-civil-liberties-by-strengthening-amici/

[39] The Constitution Project's Liberty and Security Committee, *The Case for a FISA "Special Advocate"* [see note 1].

[40] Office of the Inspector General, U.S. Department of Justice, *Review of Four FISA Applications and Other Aspects of the FBI's Crossfire Hurricane Investigation* [see note 30].

[41] Jake Laperruque, "PATRIOT Act Morass: Gains and Stalled Reforms," Project On Government Oversight, March 17, 2020. https://www.pogo.org/analysis/2020/03/patriot-act-morass-gains-and-stalled-reforms/

[42] Patel and Koreh, "Improve FISA on Civil Liberties by Strengthening Amici" [see note 38].

other relevant materials that could aid them in their advocacy before the court.[43] More broadly, improvements should be made to ensure that the amici are not simply individuals acting on their own; providing the amici with the ability to work and consult with a staff or other outside experts would significantly improve their contribution to FISA Court proceedings.

The best way to achieve these goals would be to expand the amicus role from an ad hoc role into a formal and fulltime special advocate, a measure we have long called for.[44] Doing so would improve FISA Court deliberations and help restore public confidence in the FISA Court process.

To ensure FISA Court proceedings involve more thorough deliberations, better safeguard individual rights, and have increased accountability, POGO recommends that PCLOB advocate for the expansion of the amicus role into a special advocate that:

- *is a fulltime government position, with the resources for staff of legal and technical experts;*
- *is brought in to participate in all FISA Court deliberations that raise questions about First Amendment-protected activities, civil rights, or civil liberties;*
- *is able to review or participate in FISA Title I warrant applications to ensure propriety in applications that seek to target U.S. persons;*
- *has access to all relevant materials to ensure amici can properly participate in proceedings; and*
- *has the ability to directly request that the FISA Court of Review take up decisions by the FISA Court.*

Examine the effect of this year's sunset of Section 215

In addition to the broader legal and policy issues surrounding Section 215, it is important to examine the impact of the expiration of Section 215 that occurred earlier this year. Even if this expiration is temporary, its duration has raised numerous important questions. Notably, since the March 15 expiration of Section 215—along with the roving wiretap and lone wolf authorities—the executive has publicly expressed little concern or desire to urgently restore these authorities. This raises several important questions that PCLOB should seek to understand and resolve.

First, it is essential to confirm that the executive is not attempting to reconstitute the unauthorized surveillance programs that were begun following the September 11 attacks.

---

[43] The concept of increasing materials the amici can access has been met with objections by the Department of Justice, which claims doing so could decrease information sharing from international partners. Given the vetting and clearance requirements for amici, this objection does not carry any weight. See, Jake Laperruque, "The Justice Department's Unconvincing Explanation for Its Reversal on FISA," *Lawfare*, May 29, 2020.
https://www.lawfareblog.com/justice-departments-unconvincing-explanation-its-reversal-fisa

[44] The Constitution Project's Liberty and Security Committee, *The Case for a FISA "Special Advocate"* [see note 1].

Assertion of unilateral executive authority to collect communication and business records was a gross violation of constitutional limits in the early 2000s, and would be even more so now given the additional limits Congress has imposed in recent years. In 2017, then-nominee for attorney general Jeff Sessions said that the limits Congress enacted preclude the executive from resuming the Terrorist Surveillance Program.[45] However, inquiries by senators in July 2020 to confirm that the president is not currently asserting Article II authority to enact a collection system in lieu of Section 215 remain unanswered.[46]

Second, there needs to be clarity regarding how broadly the executive believes it is able to use Section 215 for ongoing investigations. Foreign intelligence investigations can focus on large organizations and entities, and have long-running objectives beyond prosecutions. Because of this, it is possible that Section 215 is connected to investigations that will continue far longer than a standard criminal investigation. The sunset provision of FISA surveillance authorities will have little value if such investigations allow Section 215 to effectively become a "zombie surveillance authority" that is broadly used long after it officially expires.

POGO recommends that PCLOB:

- *examine and report on whether the executive branch has considered or invoked unilateral executive authority to conduct records collection activities in place of collection that would be conducted pursuant to Section 215;*
- *examine and report on whether relevant investigations are framed so broadly as to allow a meaningful portion of Section 215 to remain in use for an indefinite period of time;*
- *examine and report on what, if any, impact the expiration of Section 215 has had on intelligence community operations and investigative needs; and*
- *examine and report on whether the lone wolf authority has ever been used, whether its expiration has in any way impacted intelligence community operations and investigations, and if there is any evidence that it provides value.*

[45] *Attorney General Nomination: Hearing Before the Senate Committee on the Judiciary*, 115th Cong. (January 10, 2017). https://www.judiciary.senate.gov/meetings/01/10/2017/attorney-general-nomination

[46] Letter from Senators Patrick Leahy and Mike Lee to Attorney General William Barr and Director of National Intelligence John Ratcliffe on potential resumption of Article II unilateral executive surveillance, July 21, 2020. https://www.leahy.senate.gov/imo/media/doc/Leahy_Lee-Letter_to_Barr_and_Ratcliffe_re_FISA-072120.pdf