TESTIMONY OF JEFF KOSSEFF

ASSISTANT PROFESSOR, CYBER SCIENCE DEPARTMENT

UNITED STATES NAVAL ACADEMY

BEFORE THE UNITED STATES HOUSE OF REPRESENTATIVES JUDICIARY COMMITTEE

"SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT"

MARCH 1, 2017

Mr. Chairman, Mr. Ranking Member, and Members of the Committee, thank you for the opportunity to testify about Section 702 of the FISA Amendments Act.

My name is Jeff Kosseff, and I am an assistant professor in the United States Naval Academy's Cyber Science Department, where I teach cybersecurity law and policy. The views that I express at today's hearing are only my own, and do not necessarily represent the Naval Academy, Department of Navy, or Department of Defense. Additionally, I will note that my views are limited to the constitutionality of Section 702 as stated in the statute and explained in the public record; I have not worked in the intelligence community and therefore have no additional operational knowledge about the implementation of Section 702.

Some of my testimony today is drawn from a Hoover Institution paper[1] that I published last year with my colleague in the Naval Academy's Cyber Science Department, Chris Inglis, who served as the deputy director of the National Security Agency from 2006 to 2014.

I initially was hesitant to work on a paper about Section 702 of the FISA Amendments Act with the former head civilian executive of the NSA. As a lawyer, I have represented media organizations that were sometimes adverse to government agencies. Before becoming a lawyer, I was a journalist for more than seven years. I suspect the Committee would agree that journalists are an especially skeptical bunch, and that trait has stuck with me. I was highly skeptical about the constitutionality of a government surveillance program that I understood primarily through reading the media accounts of the Edward Snowden leaks, in which it initially was reported that the NSA and FBI "are tapping directly into the central servers of nine leading U.S. Internet companies, extracting audio, video, photographs, e-mails, documents, and connection logs that enable analysts to track a person's movements and contacts over time."[2]

Nonetheless, I evaluated the entirety of the program, based not only on media reports but also on the public primary source record. I examined publicly available information, including documents produced by the intelligence community, Foreign Intelligence Surveillance Court opinions, Congressional testimony, and the remarkably thorough report on Section 702 written by the Privacy and Civil Liberties Oversight Board (PCLOB).[3] As I will explain further, despite my initial skepticism, I found a program that is substantially different from the massive dragnet operation portrayed in the media reports. I discovered an effective foreign intelligence program that is subject to rigorous oversight by the three branches of government and, under the totality of the circumstances, complies with the Fourth Amendment.

---

[1] Chris Inglis & Jeff Kosseff, IN DEFENSE OF FAA SECTION 702: AN EXAMINATION OF ITS JUSTIFICATION, OPERATIONAL EMPLOYMENT, AND LEGAL UNDERPINNINGS (Hoover Institution) (2016) (hereinafter, "Hoover Paper").

[2] Barton Gellman, *U.S. Intelligence Mining Data from Nine U.S. Internet Companies in Broad Secret Program*, WASH. POST (June 6, 2013) (later revised) (as quoted by Peter Swire, U.S. SURVEILLANCE LAW, SAFE HARBOR, AND REFORMS SINCE 2013, white paper submitted to Belgian Privacy Forum (Dec. 17, 2015) at 14.

[3] 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) (hereinafter, "PCLOB Report").

That is not to say that I easily arrived at my conclusion regarding the constitutionality of Section 702. Nor do I deny that there are some aspects of the program that raise difficult and close Fourth Amendment questions. Whenever there is the possibility of U.S. persons' communications being seized or searched by the government, the Fourth Amendment demands serious examination of the relevant privacy implications and safeguards.

For that reason, I will spend the remainder of my testimony explaining the principal factors that led to my conclusion that Section 702 comports with the Fourth Amendment. To do so, we look at the primary requirements of the Fourth Amendment: warrants supported by probable cause and reasonableness.

Fourth Amendment Warrant Requirement

Section 702 operates without court-issued warrants. The Supreme Court long has held that a search is exempt from the Fourth Amendment's warrant requirement "when special needs, beyond the normal need for law enforcement, makes the warrant and probable cause requirement impracticable."[4] Under this "special needs" exception, for instance, schools can conduct warrantless, random drug testing of school athletes.[5]

The U.S. Supreme Court never has directly decided whether foreign intelligence surveillance falls under the "special needs" exception to the warrant requirement.[6] However, the Foreign Intelligence Surveillance Court of Review has determined that foreign intelligence is a special need that is exempt from the warrant requirement in part because the purpose of foreign intelligence gathering "goes well beyond any garden-variety law enforcement objective."[7] The Foreign Intelligence Surveillance Court has concluded the foreign intelligence exception applies to Section 702, even though the program may result in the collection of communications of or concerning U.S. persons.[8] In reaching that conclusion, the Court emphasized that the national

[4] Griffin v. Wisconsin, 483 U.S. 868, 873 (1987) (internal quotation omitted).
[5] Vernonia School District 47J v. Acton, 515 U.S. 646, 653 (1995) ("We have found such 'special needs' to exist in the public school context. There, the warrant requirement 'would unduly interfere with the maintenance of the swift and informal disciplinary procedures [that are] needed,' and 'strict adherence to the requirement that searches be based on probable cause' would undercut 'the substantial need of teachers and administrators for freedom to maintain order in the schools.'") (quoting New Jersey v. T.L.O., 469 U.S. 325, 341 (1985)); *but see* Ferguson v. City of Charleston, 532 U.S. 67, 80–82 (2001) (refusing to find a special needs exception for a state hospital's involuntary drug testing of patients when "the central and indispensable feature of the policy from its inception was the use of law enforcement to coerce the patients into substance abuse treatment.").
[6] The Supreme Court stated in United States v. United States District Court (the Keith case), 407 U.S. 297 (1972) that surveillance for *domestic* security purposes requires a warrant, but explicitly left open the question of whether a warrant is required for foreign national security threats. *Id.* at 308-09, n.8, 321-22, n.20.
[7] In Re Directives, 551 F.3d 1004, 1011 (Foreign Intelligence Surveillance Court of Review 2008).
[8] *See* [Redacted Case Name], Memorandum Opinion, United States Foreign Intelligence Surveillance Court (Bates, J.) (Oct. 3, 2011) at 68.

security purpose of Section 702 collection not only well-exceeded ordinary law enforcement objectives, but also that there was a "high degree of probability that requiring a warrant" would impede the government's ability to "collect time-sensitive information" and cause harm to "vital national security interests."[9]

Accordingly, because foreign intelligence is a special need that is distinct from normal law enforcement, the Fourth Amendment does not require a warrant for Section 702.

Fourth Amendment Reasonableness

The Fourth Amendment inquiry, however, does not end upon determination that an exception to the warrant requirement applies. Even in cases in which warrants are not required, the Fourth Amendment requires an examination of the reasonableness of the search or seizure.[10] To assess reasonableness under the Fourth Amendment, courts weigh the "totality of the circumstances" of a search, balancing "on the one hand, the degree to which it intrudes upon an individual's privacy and, on the other, the degree to which it is needed for the promotion of legitimate government interests."[11]

Government Interests

The public record strongly supports the conclusion that Section 702 is an effective national security program. The NSA stated that Section 702 collection "is the most significant tool in the NSA collection arsenal for the detection, identification, and disruption of terrorist threats to the U.S. and around the world."[12]

One challenge in conducting a public-facing analysis of a classified program is the lack of unclassified information about the program's benefits. Yet, even the relatively limited amount of information that the intelligence community has publicly provided makes clear that Section 702 serves a significant public benefit. Indeed, even critics of the program rarely dispute its effectiveness.

Section 702 is key to the extraordinarily difficult task of foreign intelligence surveillance. As PCLOB observed, "the hostile activities of terrorist organizations and other foreign entities are prone to being geographically dispersed, long-term in their planning, conducted in foreign languages or in code, and coordinated in large part from locations outside the reach of the United

[9] *Id.* at 69 (internal quotation marks and citations omitted).
[10] *See* Maryland v. King, 133 S.Ct. 1958, 1970 (2013) ("Even if a warrant is not required, a search is not beyond Fourth Amendment scrutiny; for it must be reasonable in its scope and manner of execution."); In Re Directives, 551 F.3d at 1012 ("[E]ven though the foreign intelligence exception applies in a given case, governmental action intruding on individual privacy interests must comport with the Fourth Amendment's reasonableness requirement.").
[11] Wyoming v. Houghton, 526 U.S. 295, 300 (1999).
[12] National Security Agency, THE NATIONAL SECURITY AGENCY: MISSIONS, AUTHORITIES, OVERSIGHT, AND PARTNERSHIPS (Aug. 9, 2013).

States."[13] Section 702 provides a valuable tool for the U.S. government to collect foreign intelligence information that traverses communications infrastructure in the United States.

To understand the operational benefits of Section 702, it is helpful to consider the primary alternative method to the program: obtaining a Foreign Intelligence Surveillance Court order under Title I of FISA. Because Title I was designed to protect subjects who are U.S. persons, the government must demonstrate probable cause to believe that "the target of the electronic surveillance is a foreign power or an agent of a foreign power[.]"[14] As Matthew G. Olsen, former director of the National Counterterrorism Center, testified before Congress last year, due to the growing number of foreign intelligence targets located overseas, "it was not practical to obtain individualized court orders on a routine basis."[15] Moreover, individuals are increasingly likely to have multiple email addresses and phone numbers, and are known to engage in the practice of changing them frequently, making it difficult to obtain individualized approval for each "selector."[16] Simply put, Section 702 is more nimble and better suited to modern communications infrastructure, when the communications of non-U.S. persons who are located outside of the United States may pass through the United States.[17]

After its careful review of Section 702, PCLOB concluded that the statute "has led the government to identify previously unknown individuals who are involved in international terrorism[,]"[18] and that, as of the time of the PCLOB report's drafting, more than 25 percent of NSA's reports about international terrorism relied at least in part on information gathered under Section 702.[19]

The concrete benefits of Section 702 are evident in the few declassified examples of how the government has used Section 702 data. For instance, the government used Section 702 information to arrest a man who had planned to attack a Danish newspaper that had printed cartoons of the Prophet Muhammad.[20] As a recent Heritage Foundation report summarized, "the fact remains that current and former intelligence officials, members from both political parties across two Administrations, national security law experts in the private sector, and the PCLOB

---

[13] PCLOB Report at 92.
[14] 50 U.S.C. § 1805(a)(2)(A).
[15] Testimony of Matthew G. Olsen, Hearing before the Senate Committee on the Judiciary (May 10, 2016) at 7.
[16] *See* Hoover Paper at 5 ("[I]t introduced a significant challenge for intelligence services which, under FISA 1978, had to obtain explicit approval for each and every selector they wanted to target. In 2008, there was a growing body of evidence that terrorists were making effective use of this agility, acquiring and shedding e-mail addresses and telephone numbers faster than US intelligence services could prepare, submit, and obtain required selector-by-selector approval.").
[17] *Id.* (describing "the transformation of technology between 1978 and 2008 during which time the vast portion of international communications (between nations) made a dramatic shift to physical cables (especially high-speed fiber optic cables) and domestic communications made increasing use of wireless modes of transmission.").
[18] PCLOB Report at 108.
[19] *Id.* at 10.
[20] House Committee on Intelligence, FOUR DECLASSIFIED EXAMPLES FROM THE NSA; *available at* http://intelligence.house.gov/sites/intelligence.house.gov/files/documents/50attacks.pdf.

maintain that 702 has been and continues to be a very important intelligence tool for overseas intelligence collection."[21]

In short, even based on the limited amount of information in the public record, it is clear that Section 702 serves a vital national security interest. As an outside observer and academic, I urge the intelligence community to work to declassify additional examples of the practical use of Section 702 so that the general public can better understand the role that the program plays in national security.

Invasion of Privacy Interests

Having examined the government's interest, we must turn to the other side of the Fourth Amendment balancing test and assess the invasion of individual privacy interests. I agree with the growing consensus that individuals enjoy a Fourth Amendment reasonable expectation of privacy in their electronic communications.[22]

For Fourth Amendment reasonableness purposes, the question is not merely whether individuals have a privacy interest in the materials searched or seized; the analysis focuses on the extent of the government's *invasion* of those interests.

To understand the degree of privacy invasion caused by Section 702, it is first useful to look at the many significant statutory limitations. The statute explicitly prohibits the government from using Section 702 to intentionally target: (1) "any person known at the time of acquisition to be located in the United States"[23] or (2) "a United States person reasonably believed to be located outside the United States."[24] Section 702 bars the government from intentionally targeting an individual who is located outside of the United States with the ultimate goal of collecting information from a person who is reasonably believed to be located in the United States (a practice known as "reverse targeting").[25] Section 702 also prohibits the government from intentionally acquiring "any communication as to which the sender and all intended recipients

---

[21] Paul Rosenzweig, et al., HERITAGE FOUNDATION, MAINTAINING AMERICA'S ABILITY TO COLLECT FOREIGN INTELLIGENCE: THE SECTION 702 PROGRAM (May 13, 2016).

[22] *See* United States v. Warshak, 631 F.3d 266, 286 (6th Cir. 2010) ("It follows that email requires strong protection under the Fourth Amendment; otherwise, the Fourth Amendment would prove an ineffective guardian of private communication, an essential purpose it has long been recognized to serve."); United States v. Jones, 132 S. Ct. 945, 957 (2012) (Sotomayor, J., concurring) ("[I]t may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties. This approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks. People disclose the phone numbers that they dial or text to their cellular providers; the URLs that they visit and the e-mail addresses with which they correspond to their Internet service providers; and the books, groceries, and medications they purchase to online retailers.") (internal citations omitted).

[23] 50 U.S.C. § 1881a(b)(1).

[24] 50 U.S.C. § 1881a(b)(3).

[25] 50 U.S.C. § 1881a(b)(2).

are known at the time of the acquisition to be located in the United States."[26] Moreover, the Government must acquire data under Section 702 in a manner that is "consistent" with the Fourth Amendment.[27]

Further, Section 702 explicitly requires reasonable procedures "to minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information."[28] Each agency that has access to Section 702 data has developed detailed minimization procedures.[29]

Section 702 programs are subject to a number of additional procedural safeguards:

First, and most importantly, all three branches of government oversee Section 702. Within the executive branch, the NSA imposes multiple levels of controls on the analysts who target and task communications.[30] Additionally, the Justice Department and Office of the Director of National Intelligence regularly review documentation of NSA analysts' Section 702 activities to ensure compliance.[31] Congress has an active oversight role, with the House and Senate Judiciary and Intelligence Committees receiving regular compliance reviews, certifications, and information related to other key operational aspects of Section 702.[32] Finally, the Foreign Intelligence Surveillance Court, comprised of Article III, life-tenured judges, provides extensive oversight of the program. For instance, in response to a 2011 FISC opinion questioning the sufficiency of certain minimization procedures, NSA revised those procedures.[33] The involvement of all three branches of government in the oversight of this program weighs heavily in any Fourth Amendment analysis.[34]

---

[26] 50 U.S.C. § 1881a(b)(4).
[27] 50 U.S.C. § 1881a(b)(5).
[28] 50 U.S.C. § 1801(h)(1).
[29] For redacted, declassified versions of the minimization procedures implemented by the NSA, FBI, CIA, and NCTC in 2015, see Office of the Director of National Intelligence, IC on the Record, RELEASE OF 2015 SECTION 702 MINIMIZATION PROCEDURES (Aug. 11, 2016), *available at* https://icontherecord.tumblr.com/post/148797010498/release-of-2015-section-702-minimization.
[30] *See* Hoover Paper at 16-17. The NSA and FBI each have targeting procedures, but PCLOB concluded that the NSA's targeting procedures "take primary importance because only the NSA may initiate Section 702 collection" and the FBI's targeting procedures "are applied to certain selectors only after the NSA has previously determined under the NSA targeting procedures that those selectors qualify for Section 702 targeting." PCLOB Report at 42. FBI and CIA may "nominate" targets to the NSA. *Id.*
[31] *See* Hoover Paper at 17-18.
[32] *See* PCLOB Report at 76-77; 50 U.S.C. § 1881f.
[33] Hoover Paper at 19.
[34] *See* PCLOB Report at 92 ("Where, as here, 'the powers of all three branches of government – in short, the whole of federal authority' – are involved in establishing and monitoring the parameters of an intelligence-gathering activity, the Fourth Amendment calls for a different

Second, the Attorney General and Director of National Intelligence must annually certify the purposes of Section 702 operations, and they must attest that "a significant purpose of the acquisition is to obtain foreign intelligence information."[35]

Third, before NSA collects any data through Section 702 from service providers or other companies, it must go through a detailed, multi-step targeting procedure, approved by the Foreign Intelligence Surveillance Court, to ensure that the target of the surveillance is a non-U.S. person.[36] As documented in the PCLOB report, the Justice Department "determined that 0.4% of NSA's targeting decisions resulted in the tasking of a selector that, as of the date of tasking, had a user in the United States or who was a U.S. person."[37] Only after the NSA has targeted, selected, and tasked the communications to service providers will government agencies even have the ability to query any of the data.

Fourth, the government is subject to strict retention and destruction procedures. For example, under the NSA's minimization procedures, if a communication is determined to be a domestic communication, that communication and the entire Internet transaction on which it is contained "will be promptly destroyed upon recognition" unless the NSA Director or Acting Director issues a specific written determination for each communication that the "sender or intended recipient of the domestic communication had been properly targeted under Section 702" *and* at least one of the following conditions is met: (1) the communication is "reasonably believed to contain significant foreign intelligence information;" (2) the communication is "reasonably believed to contain evidence of a crime that has been, is being, or is about to be committed;" (3) the communication is "reasonably believed" to contain technical data base information or information "necessary to understand or assess a communications security vulnerability;" or (4) the communication contains information of an "imminent threat of serious harm to life or property."[38]

Despite these safeguards, critics raise a number of legitimate points regarding potential privacy intrusions under Section 702. I will address what I believe raises the closest Fourth Amendment issue: the FBI's subsequent querying of data that has been validly collected under Section 702's targeting and minimization procedures. After reviewing extensive documentation related to Section 702, the prospect of post-collection queries for evidence of crimes causes me the greatest Fourth Amendment concerns.

The FBI's 2015 minimization procedures permit authorized FBI users to "query FBI electronic and data storage systems that contain raw FISA-acquired information to find, extract, review, translate, and assess whether such information reasonably appears to be foreign intelligence

---

calculus than when the executive branch acts alone.") (quoting United States v. Abu-Jihaad, 630 F.3d 102, 121 (2d. Cir. 2010)).

[35] 50 U.S.C. § 1881a(g)(2)(v).

[36] *See* Hoover Paper at 10-11; PCLOB Report at 44.

[37] PCLOB Report at 44-45 ("The purpose of the review was to identify how often the NSA's foreignness determinations proved to be incorrect. Therefore, the DOJ's percentage does not include instances where the NSA correctly determined that a target was located outside the United States, but post-tasking, the target subsequently traveled to the United States.").

[38] NSA 2015 Minimization Procedures at 12-13.

information, to be necessary to understand foreign intelligence information or assess its importance, or to be *evidence of a crime*."[39] The procedures require that "[t]o the extent reasonably feasible, authorized users with access to raw FISA-acquired information must design such queries to find and extract foreign intelligence information or evidence of a crime" and maintain records of all such queries.[40]

In a Nov. 6, 2015 opinion (released in redacted form to the public in April 2016),[41] Judge Thomas F. Hogan of the Foreign Intelligence Surveillance Court ruled that this process is constitutional during his review of Section 702 certifications and procedures. Judge Hogan only reached that conclusion after hearing thoughtful arguments from court-appointed Amicus Curiae. Amicus argued that under these procedures, "the FBI may query the data using U.S. person identifiers for purposes of any criminal investigation or even an assessment" and that "[t]here is no requirement that the matter be a serious one, nor that it have any relation to national security."[42] Amicus raises a strong criticism of the program: should the FBI be permitted to query the records of a *foreign intelligence* surveillance program for evidence of a crime that might be unrelated to national security?

For Fourth Amendment purposes, the answer to that question largely hinges on precisely which action is being subjected to the reasonableness test. Amicus argued that each FBI query of Section 702 information is a "separate action subject to the Fourth Amendment reasonableness test."[43] Judge Hogan correctly rejected that formulation,[44] and instead adopted the government's proposed test that "the program as a whole" must be evaluated for Fourth Amendment reasonableness.[45] Under this framework, the court must "weigh the degree to which the government's implementation of the applicable targeting and minimization procedures, viewed as a whole, serves its important national security interests against the degree of intrusion on Fourth Amendment-protected interests that results from that implementation."[46]

---

[39] FBI 2015 Minimization Procedures at 11 (emphasis added).
[40] *Id.*
[41] [Redacted Case Title], Memorandum Opinion and Order, Foreign Intelligence Surveillance Court (Nov. 6, 2015), *available at* https://www.dni.gov/files/documents/20151106-702Mem_Opinion_Order_for_Public_Release.pdf (hereinafter, "Hogan Opinion").
[42] *Id.* at 39.
[43] *Id.* at 40.
[44] *See* David S. Kris, *Trends and Predictions in Foreign Intelligence Surveillance: The FAA and Beyond*, 8 J. NAT'L SECURITY L. & POL'Y __ (forthcoming 2016) ("Underlying this debate is an interesting, although somewhat technical, question of whether querying should be seen as a separate, stand-alone Fourth Amendment event, such that it must satisfy constitutional requirements on its own, or whether it is instead best seen as part of the overall Fourth Amendment even described by the FAA, which includes but is not limited to acquisition, retention, querying, and dissemination of information. The former seems to have some support in the historical position of the government going back to the 1980s, but the latter is at least arguably more consistent with more recent authority, particularly in the context of FAA § 702.").
[45] Hogan Opinion at 40-41.
[46] *Id.* at 41.

Applying this analytical framework, Judge Hogan set forth a compelling case as to why national security interests outweigh the intrusion on individual privacy interests. Importantly – and often overlooked in Section 702 debates – is the fact that the FBI and other agencies only can query data that has been obtained through NSA's targeting program. And NSA only can obtain that data if it takes steps "to determine that the user of the selector is a non-United States person who is reasonably believed to be located outside the United States and that he or she is expected to possess, receive, or communicate foreign intelligence information."[47]

Judge Hogan's decision critically relied on the fact that "only a subset" of the Section 702 information is available to the FBI for queries.[48] Importantly, the FBI does not receive unminimized information obtained through NSA's upstream collection process, which is more likely than PRISM to contain non-target communications of U.S. persons or persons located in the United States because upstream collection can include selectors that are found in the body of a communication.[49] Moreover, Judge Hogan wrote that the government has stated that "FBI queries designed to elicit evidence of crimes unrelated to foreign intelligence rarely, if ever, produce responsive results from the Section 702-acquired data."[50]

Therefore, Judge Hogan concluded that "the risk that the results of such a query will be viewed or otherwise used in connection with an investigation that is unrelated to national security appears to be remote, if not entirely theoretical."[51] However, he recognized the need for the Court "to reassure itself that this risk assessment is valid," and therefore began requiring the government to report "any instance in which FBI personnel receive and review Section 702-acquired information that the FBI identifies as concerning a United States person in response to a query that is not designed to find and extract foreign intelligence information."[52] This strikes me as an appropriate safeguard to protect against abuse of the program, and it demonstrates the efficacy of FISC oversight of Section 702.

Similarly, in 2015, a federal judge in Colorado declined to suppress Section 702 evidence in a criminal case against Jamshid Muhtorov, who was charged with providing material support to a designated terrorist organization and conspiracy to do the same.[53] Although Muhtorov challenged a variety of aspects of Section 702, much of his challenge related not to the initial, incidental collection of his communications, but to the subsequent "retention and *use* of those communications by federal law enforcement in criminal proceedings against him in a court of law."[54] Judge John L. Kane explained why this subsequent use is not a discrete "search" under the Fourth Amendment:

---

[47] *Id*.
[48] *Id.* at 43.
[49] PCLOB Report at 35-41; Hogan Opinion at 43-44 (observing that upstream collection is "more likely than others to include non-target communications of United States persons and persons located in the United States that have no foreign intelligence value.")
[50] Hogan Opinion at 44.
[51] *Id.*
[52] *Id.*
[53] United States v. Muhtorov, Criminal Case No. 12-cr-00033-JLK (D. Colo. Nov. 19, 2015).
[54] *Id.* at 29 (emphasis in original).

> Accessing stored records in a database legitimately acquired is not a search in the context of the Fourth Amendment because there is no reasonable expectation of privacy in that information. Evidence obtained legally by one police agency may be shared with similar agencies without the need for obtaining a warrant, even if it sought to be used for an entirely different purpose.[55]

On balance, the FBI's ability to query Section 702 data, as described in the public record, does not render Section 702 unconstitutional. During the reauthorization process, Congress may well conclude that there are legitimate policy reasons to limit the FBI's ability to conduct such queries. However, my testimony today is limited to the application of the Fourth Amendment to Section 702.

Concluding Thoughts

On balance, the important role that Section 702 plays in promoting national security outweighs the intrusions on individual privacy interests. As I stressed at the beginning of my testimony, I did not arrive at this conclusion easily. Indeed, there are many close cases in which strong constitutional arguments can be made for and against elements of the program, most notably when domestic law enforcement subsequently queries Section 702 data for evidence of ordinary crimes. As a matter of Fourth Amendment law, however, we must examine the totality of the program. Section 702 contains vital safeguards, including oversight by this Committee and others as well as the Foreign Intelligence Surveillance Court. Indeed, after its extensive examination of Section 702, PCLOB concluded that "[o]peration of the Section 702 program has been subject to judicial oversight and extensive internal supervision, and the Board has found no evidence of intentional abuse."[56]

I recognize that the Committee is conducting a hearing on Section 702 in the year when it is set to expire, and you likely have many policy options to consider. I am limiting my comments today to whether Section 702 is constitutional, and the other panelists may be better positioned to comment on policy preferences.

I will conclude with one broad observation about the importance of transparency. The intelligence community continues to increase the amount of information available to the public about Section 702, including statistics about the use of Section 702, redacted Foreign Intelligence Surveillance Court Opinions, and minimization procedures.[57] I commend these transparency efforts, which are especially important in supporting an informed public legal and policy debate in the context of foreign intelligence programs that are inherently secretive and classified. Further, the work of PCLOB has been absolutely essential in informing the public debate on Section 702. Indeed, without PCLOB's thorough and transparent evaluation of Section 702, it would be difficult, if not impossible, to evaluate the constitutionality of Section 702. I hope that these transparency efforts continue, because they allow all of us to better do our job at evaluating these vital constitutional issues. The Fourth Amendment – like other important

---

[55] *Id.* at 31.
[56] PCLOB Report at 2.
[57] *See* OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE, IC ON THE RECORD, *available at* https://icontherecord.tumblr.com/.

constitutional rights – is highly fact-dependent and requires close analysis of not only how the program is structured by statute, but how it actually is implemented. The public release of information by the intelligence community and public hearings such as this are absolutely vital as we continue to evaluate Section 702 and other intelligence programs.

National Security Archive,

Suite 701, Gelman Library, The George Washington University,

2130 H Street, NW, Washington, D.C., 20037,

Phone: 202/994-7000, Fax: 202/994-7005, nsarchiv@gwu.edu