The Heritage Foundation

BACKGROUNDER

No. 3122 | MAY 13, 2016

Maintaining America's Ability to Collect Foreign Intelligence: The Section 702 Program

David R. Shedd, Paul Rosenzweig, and Charles D. Stimson

Abstract

Section 702 of the Foreign Intelligence Surveillance Act will come up for reauthorization in 2017. The Section 702 program targets non-U.S. persons reasonably believed to be located outside the United States, in order to acquire foreign intelligence. Over the past several years, this surveillance of the online activities of foreigners has been an invaluable source of information for American intelligence professionals and officials. Some say that more than 25 percent of all current U.S. intelligence is based on information collected under Section 702. Still, critics believe that the program infringes on Americans' rights. Their concern hinges on the inevitable reality that in the course of collecting information about foreign actors, the Section 702 program will also collect information about American citizens. As a result, some opponents liken the Section 702 program to the government telephony metadata program disclosed by Edward Snowden, and characterize Section 702 as an instance of government overreach. Such comparisons are misguided. The program is so vital to America's national security that Congress should reauthorize Section 702 in its current form.

Section 702 of the Foreign Intelligence Surveillance Act (FISA) will, in its current form, come up for reauthorization in 2017. Broadly speaking, the Section 702 program targets non-U.S. persons reasonably believed to be located outside the United States, in order to acquire foreign intelligence. Over the past several years, this surveillance of the online activities of foreigners has been a critical and invaluable tool for American intelligence professionals and officials. Knowledgeable officials note that more than 25 per-

Key Points

- Section 702 of the Foreign Intelligence Surveillance Act (FISA) will come up for reauthorization in 2017. The Section 702 program targets non-U.S. persons located overseas in order to acquire foreign intelligence.
- This surveillance of the online activities of foreigners has been an invaluable source of information for American intelligence professionals and officials. More than 25 percent of all current U.S. intelligence is based on information collected under Section 702.
- Still, there are critics who believe that the program infringes on Americans' rights due to the inevitable reality that in the course of collecting information about foreign actors, the Section 702 program will also collect information about American citizens.
- Far from being a matter of government overreach, however, the program is so vital to America's national security that Congress should reauthorize Section 702 in its current form.

This paper, in its entirety, can be found at **http://report.heritage.org/bg3122**

The Heritage Foundation
214 Massachusetts Avenue, NE
Washington, DC 20002
(202) 546-4400 | heritage.org

Nothing written here is to be construed as necessarily reflecting the views of The Heritage Foundation or as an attempt to aid or hinder the passage of any bill before Congress.

cent of all current U.S. intelligence is based on information collected under Section 702.[1]

Still, there are those who have concerns about the program. These critics believe that the program, as currently implemented, infringes on Americans' rights. Their concern hinges on the inevitable reality that in the course of collecting information about foreign actors, the Section 702 program will also collect information about American citizens. As a result, some opponents liken the Section 702 program to the government telephony metadata program disclosed by Edward Snowden, and characterize Section 702 as an instance of government overreach.[2] Such comparisons are misguided and unfair. The program is so vital to America's national security that Congress should reauthorize Section 702 in its current form.

Section 702 Explained

Section 702 has its origins in President George W. Bush's terrorist surveillance program and the PATRIOT Act. That program was initiated in the immediate aftermath of the 9/11 terror attacks, on the President's own authority. That reliance on exclusive presidential authority contributed to the controversy that initially attended the program—some vocal critics saw it as an example of executive overreach.

That aspect of the criticism was significantly ameliorated, if not eliminated, several years later, when Congress fully discussed and authorized the activities in question. Indeed, the governing law was adopted and amended twice, after the program had been initiated on the President's own authority. First, Congress adopted a temporary measure known as the Protect America Act in 2007.[3] Then, it passed the FISA Amendments Act (FAA) in 2008. This is the statute that includes the new Section 702.[4]

Under Section 702, the U.S. Attorney General and the Director of National Intelligence (DNI) may jointly authorize surveillance of people who are not "U.S. persons." U.S. persons is a term of art in the intelligence community (IC) that means people who are not only American citizens but also covers permanent-resident aliens. As such, the targets of Section 702 surveillance can be neither citizens nor permanent residents of the U.S.

Section 702 authorizes the government to acquire foreign intelligence by targeting non-U.S. persons "reasonably believed" to be outside U.S. borders. Taken together, these two requirements identify the fundamental domain of Section 702 surveillance: it applies to foreigners on foreign soil. It is expressly against the law to attempt collection of information from targets inside the U.S.—whether Americans or foreigners—or to deliberately target the collection of online communications of American citizens.[5]

The law also requires the government to develop "targeting procedures"—the steps the government needs to take in order to ensure that the target is outside the United States at any time that electronic surveillance is undertaken. Obviously, that is sometimes difficult. A cell phone number, for instance, remains the same whether the phone is physically overseas or in the U.S., and the fact that someone has a U.S. cell phone number does not necessarily indicate whether the owner or user of that cell phone is a foreigner or an American. Hence, targeting must be tied to the geolocation of a phone and some knowl-

1. Privacy and Civil Liberties Oversight Board, Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act report of July 2, 2014, p. 10: "Presently, over a quarter of the NSA's reports concerning international terrorism include information based in whole or in part on Section 702 collection, and this percentage has increased every year since the statute was enacted."
2. The telephony metadata program, also sometimes known as the Section 215 program after the section of the PATRIOT Act which authorized it, was substantially revised by Congress, due in large part to these types of concerns. USA Freedom Act of 2015, https://judiciary.house.gov/issue/usa-freedom-act/ (accessed April 14, 2016). For a summary of Heritage analysts' views on Section 215, see James J. Carafano, Charles D. Stimson, Steven Bucci, John Malcolm, and Paul Rosenzweig, "Section 215 of the PATRIOT Act and Metadata Collection: Responsible Options for the Way Forward," Heritage Foundation *Backgrounder* No. 3018, May 21, 2015, http://www.heritage.org/research/reports/2015/05/section-215-of-the-patriot-act-and-metadata-collection-responsible-options-for-the-way-forward. Section 215 of the PATRIOT Act and Section 702 of FISA differ vastly in scope, scale, intent, and effect; hence, the analogy is a flawed one.
3. Protect America Act of 2007, P.L. 110–55.
4. FISA Amendments Act of 2008, P.L. 110–261.
5. This distinction is one of the things that makes the 702 program different from its much better known cousin, the Section 215 metadata program. Section 215 did not collect the content of communications, only the metadata—such as phone numbers called, and the dates and lengths of calls. However it, quite explicitly, was designed to collect information about Americans and about events occurring on American soil.

edge about the owner/user, rather than solely to the phone's number. Ultimately, it is the targeting procedures, not the targets themselves, that must be approved by the U.S. Foreign Intelligence Surveillance Court (FISC).[6]

To conduct this surveillance, the government can compel assistance from Internet service providers (ISPs) and telephone companies in acquiring foreign intelligence information—that is, information relating to a foreign espionage program or international terrorism. The government often compensates these providers for the necessary effort. According to *The Washington Post*, the payments range from $250 million to nearly $400 million annually.[7] Some critics of the program suspect that as a result, surveillance turns from a legal obligation to a source of income. Finally, it is important to note that not only regulated carriers, such as traditional cable and telephone companies (such as AT&T or Verizon), are required to participate, but also newer technology companies to include Google, Facebook, and Skype.

The Incidental Collection Issue

If that were all that the 702 program involved, it would likely not be particularly controversial. Few Americans have expressed grave concerns about America's overseas intelligence collection. Significantly, the 702 program cannot be used to target any U.S. person or any person located in the U.S., whether that person is an American or a foreigner. The government is also prohibited from "reverse targeting" under 702—that is, the government cannot target a non-U.S. person outside the U.S. when the real interest is to collect the communications of a person in the U.S. or of any U.S. person, regardless of location.

But a residual issue arises because of the inevitability of inadvertent collection—the incidental collection of information about Americans as part of the authorized collection of foreign intelligence.

To see why this happens, one needs to understand two distinct aspects of the Section 702 program: one portion that goes by the name of PRISM, and another that is referred to colloquially as "upstream collection."[8]

PRISM collection is relatively straightforward. A hypothetical can explain: The government has information about a particular e-mail address, or a particular individual, linking it or him to a foreign terrorist organization. That address (john.doe@xyz.com) or that individual's name (John Doe) is known as a "selector"; it is a basis for sifting through vast quantities of data, and selecting what will be collected and analyzed.

The Attorney General and the DNI certify the selector as relating to a non-U.S. person who is outside the United States, and who is reasonably believed to be connected to a foreign intelligence activity. Then, the National Security Agency (NSA) sends a query about that selector to an ISP. The ISP, in turn, is required to hand over to the government any communications it might have that were sent to—or from—the identified selector. The NSA receives all data collected through PRISM, and makes portions of it available to the CIA and the FBI.

Upstream collection, by contrast, does not focus on the ISP. Instead, it focuses on the "backbone," through which all telephone and Internet communications travel, which lies "upstream" within the telecommunications infrastructure. For example, an individual's ISP might be a local company, while the backbone that carries its Internet traffic across the ocean to Europe is almost certainly operated by a larger provider, such as Verizon or AT&T.

There are several additional differences that distinguish upstream collection from PRISM. Most notably, upstream collection can involve "about" communications. "About" communications refer to selectors that occur within the content of the monitored communication, instead of, in the example of e-mail, in the "To" or "From" line.

So, if the government were using a name—John Doe—as a selector, under the upstream collec-

6. The Foreign Intelligence Surveillance Court (FISC) "entertains applications made by the United States Government for approval of electronic surveillance, physical search, and certain other forms of investigative actions for foreign intelligence purposes," United States Foreign Intelligence Surveillance Court, http://www.fisc.uscourts.gov/ (accessed April 14, 2016).
7. Craig Timberg and Barton Gellman, "NSA Paying U.S. Companies for Access to Communications Networks," *The Washington Post*, April 29, 2013, https://www.washingtonpost.com/world/national-security/nsa-paying-us-companies-for-access-to-communications-networks/2013/08/29/5641a4b6-10c2-11e3-bdf6-e4fc677d94a1_story.html (accessed March 8, 2016).
8. Much of the description that follows is derived from the report on the Section 702 program produced by the President's Civil Liberties and Oversight Board (PCLOB) dated July 2, 2014.

tion program, it would also collect foreign intelligence–related communications in which that name appeared in the body of the communication. Say, for example, that two al-Qaeda members are communicating via e-mail, and one says to the other: "We should recruit Doe." That e-mail would be subject to upstream collection and would be a good example of an "about" communication. The e-mail is *about* Doe. Under the PRISM program, by contrast, the government would collect e-mails to and from the user name, and nothing more.

As should be evident, in some cases, these programs might result unintentionally in the collection of information about an American. If two Americans are communicating domestically in an exchange that names a foreign intelligence target (say, an e-mail that mentions an al-Qaeda operative by name), that e-mail might be incidentally collected by upstream collection. Likewise, an e-mail between two terrorist targets might be collected that incidentally includes information not only about legitimately identified U.S. persons (the recruit target John Doe), but also others. An e-mail might also mention Mary Doe—even though no evidence exists of any connection between Mary Doe and a foreign intelligence matter.

This prospect of collecting American data led Congress to include certain requirements that would reduce, though not entirely eliminate, the possibility that the data could be misused. Under the FAA, when information is collected about an American, whether incidentally as part of an authorized investigation, or inadvertently as the result of a mistake, the government is required to apply FISC-approved "minimization" procedures to determine whether such information may be retained or disseminated.

When lawyers and intelligence professionals use the word "minimization" in the context of intelligence collection, it means that any information inadvertently collected on a U.S. person is retained (if at all) only for a limited time, and that information about Americans is used and revealed and further disseminated only under narrowly defined circumstances. Minimization requirements may also mean deleting the information entirely. As with the targeting procedures, these minimization procedures are approved by the FISC—but again, the approval is for the entire system of minimization, not for each individual case.

So, for example, under these minimization rules, the NSA, CIA, and FBI are subject to certain limitations in how they are permitted to query and analyze the data they have lawfully collected. For example, they must demonstrate a reasonable likelihood that targeting a particular item in the information collected will result in the development of foreign intelligence. In other words, the rules limit when a U.S. person can be targeted for examination, and how long data about an American can be retained before it is deleted.

The Effectiveness of Section 702

With that background in mind, it is useful to turn to more practical questions about the program: Does it work? Is it being abused?

The public record suggests that the Section 702 program has indeed helped in the fight against terrorism. Classified records might provide additional support for this conclusion but they are unavailable to us.[9] The Privacy and Civil Liberties Oversight Board (PCLOB)—a bipartisan panel in the executive branch that reviews actions the executive branch takes to protect the country from terrorism, and also monitors civil liberty concerns—has reported that more than one-quarter of NSA reports on international terrorism include information that is based in whole, or in part, on data collected under the Section 702 program.

The PCLOB found that the 702 program "makes a substantial contribution to the government's efforts to learn about the membership, goals, and activities of international terrorist organizations, and to prevent acts of terrorism from coming to fruition."[10] Additionally, the program has "led the government to identify previously unknown individuals who are involved in international terrorism, and it has played a key role in discovering and disrupting specific terrorist plots aimed at the United States and other countries."[11]

9. The three authors of this *Backgrounder* continue to hold active security clearances and therefore relied exclusively on public authorized sources for the description of the program.
10. Privacy and Civil Liberties Oversight Board, "Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Act of 2014," p. 104.
11. Ibid., p. 10.

Although the details supporting these findings are classified, the board has also said that the program has played a role in discovering, and disrupting, specific terrorist plots aimed at the United States by enabling the government to identify previously unidentified individuals involved in international terrorism.[12] Additionally, the U.S. House of Representatives Permanent Select Committee on Intelligence (HPSCI) has posted three declassified examples from the NSA that involved the effective use of Section 702 collection in 2009: the New York City Subway Attack Plot; the Chicago Terror Investigation; and Operation Wi-Fi.

A few critics of the 702 program have disputed its actual impact in the New York City Subway Attack Plot and the Chicago Terror Investigation. *The Guardian* interviewed several people who were involved in the two investigations and reviewed U.S. and British court documents.[13] Based on this incomplete record, *The Guardian* concluded that these investigations began with "conventional" surveillance methods—such as "old-fashioned tip-offs" of the British intelligence services—rather than from leads produced by NSA surveillance.

But 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 maintain that 702 has been and continues to be a very important intelligence tool for overseas intelligence collection.

Section 702 Criticisms v. Facts

Some of the criticisms of Section 702 are little more than philosophical objections to the concept of overseas surveillance.

Setting aside those concerns, there are other specific criticisms, each of which lacks merit. For example, there has been criticism that there is no significant publicly available data on how little, or how much, incidental collection there is about U.S. persons. Such data would be helpful to know in assessing the program. According to the PCLOB, in 2013 the NSA approved 198 U.S. person identifiers to be used as content query terms. The real issue is the frequency with which U.S. persons' information was collected *incidentally* to the general foreign intelligence mission, and what is done with the information. After all, if the volume of incidental collection even remotely came close to what is collected as useful data on terrorism activities, including threats, skepticism about Section 702's efficacy would be warranted.

Given that the targets of Section 702 collection are non-U.S. persons reasonably believed to be located overseas, it can reasonably be inferred that the predominant portion of the collected data does not contain U.S. person information. Although it would be useful to have an accurate estimate of how much incidental U.S. person information actually resides within the remaining portion of the data collected under the Section 702 program, it has proved very difficult to find any solution that would provide such an estimate. The first problem is that the collected data is often not readily identifiable as being associated with a U.S. person and would require the application of additional scarce technological and analytic resources in an effort to make those associations. The second problem is that the targets of the Section 702 collection efforts do not always communicate with persons of foreign intelligence interest. Ironically, an effort to ascertain an accurate estimate of non-pertinent U.S. person information lying dormant in the collected data is inconsistent with the purpose of Section 702, which is to identify foreign intelligence information. Such an effort to provide an estimate would result in *more* invasive review of U.S. person information.

FISA itself takes a more practical approach in attempting to understand the potential U.S. person privacy implications raised by Section 702 collection. It requires the head of each element of the Intelligence Community to conduct an annual review and to provide an accounting of the references to U.S. persons in intelligence reporting.[14] This outcome-based approach focuses on the U.S. person information that is actually being seen by the Intelligence Community, in order to assess whether there is any

12. Privacy and Civil Liberties Oversight Board, "Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 2014."
13. Ed Pilkington, "Nicholas Watt, NSA Surveillance Played Little Role in Foiling Terror Plots, Experts Say," *The Guardian*, June 12, 2013, http://www.theguardian.com/world/2013/jun/12/nsa-surveillance-data-terror-attack (accessed March 8, 2016).
14. 50 U.S.C. 1881a(l)(3).

prejudicial impact on privacy rights. Also, the Office of the Director of National Intelligence (ODNI) recently released its "Statistical Transparency Report Regarding Use of National Security Authorities–Annual Statistics for Calendar Year 2015."[15] The report estimates that 94,368 non-U.S. persons are targets of Section 702 collection. By comparison, the report estimates that the IC used 4,672 known U.S. person search terms in 23,800 queries of the lawfully collected Section 702 data. The report also notes that in 2015, the NSA disseminated 4,290 Section 702 intelligence reports that included U.S. person information. Of those reports, the U.S. person information was masked in 3,168 reports and unmasked in 1,122 reports. The remaining major criticisms of the 702 program are more systematic and definitional. One critique is that the government uses too broad a means in its first stage of collection, which is then followed by a more refined collection of data.[16] Judge Thomas F. Hogan of the FISC has described the program more accurately: "While in absolute terms, the scope of acquisition under Section 702 is substantial, the acquisitions are not conducted in a bulk or indiscriminate manner. Rather they are effected through...discrete targeting decisions for individual selectors."[17]

Another complaint about the Section 702 program is that U.S. person data is retained—at least partially—at all. Under current rules, when the U.S. government targets someone abroad, it is not required to discard the incidentally collected communications of U.S. persons—if authorities conclude that those conversations constitute foreign intelligence.

In that event, even incidental conversations by or about U.S. persons may be retained. And the threshold for querying a U.S. person within the data collected is relatively low. To affirmatively query the data collected about a U.S. person, all that is needed is a determination that the search is reasonably likely to return foreign intelligence information. "Reasonably likely" is an especially easy standard to meet. It does not, for example, require any particularized suspicion that the U.S. person who is subject of the inquiry is engaged in any wrongdoing himself.

For that reason, a Presidential Review Board, as well a few Members of Congress, believe that Section 702 collection on Americans goes too far.[18] The program, they argue, is permissible and lawful without individual case supervision or a warrant requirement precisely because it targets non-Americans. So they contend that when the communications of U.S. persons are queried, probable cause and warrant requirements should apply. Any loophole that allows that particular querying should be closed because the government should not be able to obtain "back door" evidence against U.S. persons that it could otherwise only obtain with judicial approval.

But there is no "back door" here—a query does not collect any additional data. The FISC specifically holds that the 702 collection is constitutional and entirely consistent with the Fourth Amendment's protections. The court found that "the querying provisions of the FBI Minimization Procedures strike a reasonable balance between the privacy interests of U.S. persons and persons in the United States, on the one hand, and the government's national security interests, on the other."[19] Even the fact that the "FBI's use of those provisions to conduct queries designed to return evidence of crimes unrelated to foreign intelligence" did "not preclude the Court from concluding that taken together, the targeting and minimization procedures submitted with the 2015 Certifications are consistent with the requirements of the Fourth Amendment."[20]

Obviously, Congress itself did not agree with these systematic and definitional complaints. While the focus of Section 702 collection is on non-U.S. persons located overseas, one of the specifically intend-

15. Office of the Director of National Intelligence, IC on the Record, "Transparency Report: Statistical Transparency Report Regarding Use of National Security Authorities–Annual Statistics for Calendar Year 2015," May 2, 2016, https://icontherecord.tumblr.com/transparency/odni_transparencyreport_cy2015 (accessed May 6, 2016).
16. William C. Banks, "Responses to 10 Questions," *Journal of the National Security Forum*, Vol. 35, No. 5 (2009), http://open.mitchellhamline.edu/cgi/viewcontent.cgi?article=2850&context=wmlr (accessed March 8, 2016).
17. Memorandum Opinion and Order, November 6, Judge Hogan (Foreign Int. Surv.Ct. 2015), slip op., p. 45.
18. The President's Review Group on Intelligence and Communications Technologies, "Liberty and Security in a Changing World," December 12, 2013, https://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf (accessed March 8, 2016).
19. Memorandum Opinion and Order, November 6, Judge Hogan (Foreign Int. Surv.Ct. 2015), slip op., p. 44.
20. Memorandum Opinion and Order, November 6, Judge Hogan (Foreign Int. Surv.Ct. 2015), slip op., pp. 44–45.

ed benefits of Section 702 was its ability to provide tip and lead information about persons in the United States who might be conspiring with overseas terrorists. This limited information might prove useful in helping to establish the probable cause necessary to obtain full surveillance coverage of these domestic suspects. It is also important to understand that the response to complaints about the theoretical possibility of abuse under FISA revolves around tight controls. The PCLOB found little evidence of abuse of the Section 215 metadata program, and in the case of Section 702 implementation found virtually no intentional misuse of the collection authorities where U.S. persons were concerned:

> Over the years, a series of compliance issues were brought to the attention of the FISA court by the government. However, none of these compliance issues involved significant intentional misuse of the system. Nor has the Board seen any evidence of bad faith or misconduct on the part of any government officials or agents involved with the program. Rather, the compliance issues were recognized by the [FISA] court—and are recognized by the Board—as a product of the program's technological complexity and vast scope, illustrating the risks inherent in such a program.[21]

Similarly, the PCLOB included a section in its 702 report called "Compliance Issues." According to the PCLOB, the few instances of error in the administration of the 702 program were infrequent and mainly minor and administrative in nature. That is why the PCLOB found that "internal and external compliance programs have not to date identified any intentional attempts to circumvent or violate the procedures or the statutory requirements, but both unintentional incidents of noncompliance and instances where Intelligence Community personnel did not fully understand the requirements of the statute."[22]

In other words, *all* of the errors in the program were accidental or due to mistakes. *None* was the product of intentional misconduct. Indeed, the non-compliance incident rate has been substantially below 1 percent, according to the PCLOB.[23] Over half of the reported incidents involved instances in which the "NSA otherwise complied with the targeting and minimization procedures in tasking and de-tasking a selector, but failed to make a report to the NSD and ODNI" in a timely fashion.[24]

Two other common reasons why compliance errors occurred are that: (1) the wrong selector was tasked due to a typographical error, or (2) a delay in de-tasking (removing the selector) resulted when an analyst de-tasked some, but not all, of the Section 702-tasked selectors placed on a non-U.S. person target known to be traveling to the United States.[25]

Taken together, these minor administrative errors accounted for "almost 75% of the compliance incidents," according to the PCLOB.[26]

Section 702: Constitutional and Lawful

One last aspect of Section 702 needs to be addressed: the suggestion that the program might in some way be unconstitutional or unlawful. This *Backgrounder* concludes that relevant case law firmly supports the constitutionality and legality of the Section 702 program. To support this conclusion, we provide a brief history of relevant case law.

The predicate case is *United States v. United States District Court*,[27] sometimes known as the *Keith* case, after Judge Damon Keith, the federal district court judge who oversaw the case.

The case hearkens back to an era of protest and civil unrest in the United States. It involved sever-

21. 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 (accessed March 8, 2016).
22. Privacy and Civil Liberties Oversight Board, "Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 2014," p. 77.
23. Ibid.
24. Ibid., p. 78.
25. Ibid.
26. Ibid.
27. *United States v. United States District Court*, 407 U.S. 297 (1972).

al leaders of the so-called White Panther Party—a white supremacist group—who were charged with bombing a CIA office in Ann Arbor, Michigan, in 1968. Their phones were wiretapped by order of U.S. Attorney General John Mitchell, who served under President Richard Nixon. Mitchell said that no warrant was required to authorize the interception, because the defendants posed a "clear and present danger to the structure or existence of the government."

Judge Keith responded that the Attorney General's rationale was insufficient, and ruled that warrantless interception and surveillance of domestic conversations was unconstitutional. When the case reached the Supreme Court, the justices agreed with Judge Keith, establishing as precedent the idea that a warrant was needed before electronic surveillance commenced, even if the domestic surveillance was related to national security.

As Justice Lewis Powell said in writing for the Court, the "price of lawful public dissent must not be a dread of subjection to an unchecked surveillance power." Justice Powell continued, "Nor must the fear of un-authorized official eavesdropping deter vigorous citizen dissent and discussion of government action in private conversation. For private dissent, no less than open public discourse, is essential to our free society."

Notably, however, the Court limited its holding to domestic surveillance, and said that different rules might apply when the surveillance occurred outside the United States, or was directed at a foreign power—or at non-Americans. Regarding surveillance of non-Americans overseas, courts around the country have agreed with the implicit suggestion of the Supreme Court, holding that surveillance for foreign intelligence purposes need only be reasonable (and that a warrant is not required).[28] That distinction—between domestic and foreign surveillance—is preserved in FISA, which allows more relaxed FISA procedures (for which a criminal warrant was not required) only when the purpose of the investigation is to collect foreign intelligence.

In *Vernonia School District 47J v. Acton*, the Supreme Court upheld the drug testing of high school athletes and explained that the exception to the warrant requirement applied "when special needs, beyond the normal need for law enforcement, make the warrant and probable cause requirements impracticable."[29] Although *Vernonia* was not a foreign intelligence case—far from it—the principles from the Court's "special needs" cases influenced later cases in the national security context.

In "In re: Sealed Case," the United States Foreign Intelligence Surveillance Court of Review held that FISA did not require the government to demonstrate to the FISA court that its primary purpose in conducting electronic surveillance was not criminal prosecution and, significantly, the PATRIOT Act's amendment to FISA, permitting the government to conduct surveillance of agents of foreign powers if foreign intelligence was the "significant purpose" of the surveillance, did not violate the Fourth Amendment.[30] The court avoided an express holding that a foreign intelligence exception exists, but held that FISA could survive on reasonableness grounds.

In 2008, "In re: Directives Pursuant to Section 105B of FISA" applied the principles derived from the special needs cases to conclude that the foreign intelligence surveillance authorized by the Protect America Act possesses characteristics that qualify it for a foreign intelligence exception to the warrant requirement of the Fourth Amendment.[31]

Notably, the "In re: Directives" decision cites a Fourth Circuit opinion for the proposition that there is a high degree of probability that requiring a warrant would hinder the government's ability to collect time-sensitive information and thus impede vital national security interests.[32]

In April 2016, the first decision addressing the constitutionality of upstream collection under Section 702 was publicly released. The FISA court issued a declassified opinion[33] in which it concluded that use of information collected under Section 702 authority for domestic investigations satisfied

28. *United States v. Truong Dinh Hung*, 629 F.2d 908 (4th Cir. 1980).
29. 515 U.S. 646 at 653 (1995).
30. In re: Sealed Case, 310 F.3d 717, 721 (Foreign Int.Surv.Ct.Rev. 2002).
31. In re: Directives Pursuant to Section 105B of FISA, 551 F.3d 1004, 1010 (Foreign Int.Surv.Ct.Rev. 2008).
32. *U.S. v. Truong Dinh Hung,* 629 F.2d 908 at 915 (1980).
33. Memorandum Opinion and Order, November 6, Judge Hogan (Foreign Int.Surv.Ct. 2015).

both constitutional standards and was within the statutory bounds of the FISA Amendments Act. Notably, for purposes of this discussion, the court reached this conclusion after having had the benefit of a public advocate who articulated a position contrary to that of the government.[34] Judge Hogan cites "In re: Directives" in support of the proposition that the Fourth Amendment does not require the government to obtain a warrant to conduct surveillance in order "to obtain foreign intelligence for national security purposes [that] is directed against foreign powers or agents of foreign powers reasonably believed to be located outside of the United States."

Section 702: Continuing Improvements

On February 5, 2016, the PCLOB issued its "Recommendations Assessment Report." The purpose of the report was to assess whether the DNI had responded appropriately to recommendations it had made for the improvement of the program.

The DNI had taken action to the PCLOB recommendations. Indeed, with respect to the 10 recommendations relating to the Section 702 program, the PCLOB Recommendations Assessment Report determined that five recommendations have been fully implemented; one has been substantially implemented; three are in the process of being implemented; and one has been partially implemented.[35]

The historical record demonstrates the effectiveness of both the PCLOB's oversight function and the responsiveness of the DNI to its recommendations—a win-win story in the new age of intelligence oversight.[36]

Conclusions

First, Section 702 is constitutional, statutorily authorized, and carefully constructed to address a vital U.S. national security requirement: the collection of vital information relating to foreign threats.

Second, it seems clear that, in light of careful scrutiny by the PCLOB, the specter of alleged abuse of the program is more theoretical than real.

Third, the Section 702 program has great current utility and provides invaluable intelligence of practical impact and not replaceable by other means of collection.

The benefits of the Section 702 program greatly outweigh its (theoretical) costs and the program should continue as currently authorized. Indeed, the record suggests that the 702 Program is invaluable as a foreign intelligence collection tool. The fruits of the program constitute more than 25 percent of the NSA's reports concerning international terrorism. It

34. To the extent that the FISC has been criticized for being a "rubber stamp" court, the fact that the FISC invited an independent *amicus* to separately brief and challenge each aspect of the 702 program's targeting and minimization procedures directly refutes that contention.

35. Specifically, the following recommendations from the PCLOB have been implemented:

    - Update the FBI's minimization procedures to accurately reflect the Bureau's querying of Section 702 data for non-foreign intelligence matters, and place additional limits on the FBI's use of Section 702 data in such matters;
    - Periodically assess upstream collection technology to ensure that only authorized communications are acquired;
    - Examine the technical feasibility of limiting particular types of "about collection";
    - Publicly release the current minimization procedures for the CIA, FBI, and NSA; and
    - Create and submit to the FISC a single consolidated document describing all significant rules governing operation of the Section 702 program—implemented by the Executive Branch.

    The following three recommendations are in the process of being implemented:

    - Require NSA and CIA personnel to provide a statement of facts explaining their foreign intelligence purpose before querying section 702 data using U.S. person identifiers, and develop written guidance on applying this standard;
    - Adopt measures to document and publicly release information showing how frequently the NSA acquires and uses communications of U.S. persons and people located in the United States; and
    - Develop a methodology to assess the value of counterterrorism programs.

    The following recommendation has been substantially implemented:

    - Provide the FISC with documentation of Section 702 targeting decisions and U.S. person queries.

    The following recommendation has been implemented in part:

    - Revise NSA procedures to better document the foreign intelligence reason for targeting decisions.

36. The PCLOB also made several recommendations with respect to the Section 215 program. Those, as well, have generally been fully implemented.

has clearly defined implementation rules and robust oversight by all three branches of government, and is a necessary tool for defending the nation.

Congress should reauthorize 702 in its entirety. There is no need for a further sunset of the act's provisions, as it has demonstrated its usefulness; and an arbitrarily forced reconsideration by Congress is unnecessary, a waste of time and money, and at the expense of national security.

The program can, and should, be implemented in a manner that is consistent with American values. To quote General Michael Hayden, former director of the NSA and former CIA director:

> [A]n American strategy for cyberspace must reflect and serve our ideals. In our zeal to secure the internet, we must be careful not to destroy that which we are trying to preserve, an open, accessible, ubiquitous, egalitarian, and free World Wide Web. There are nations—like Iran, China, Russia and others—who view precisely those attributes as the very definition of cyber security threats. Their concern is not digital theft, but the free movement of ideas. We must take care that in our efforts to prevent the former, we do not legitimize their efforts to prevent the latter.[37]

A properly configured Section 702 program has met that challenge to the benefit of the American public. At a time when international terrorism is on the rise, the United States must have a lawful, robust foreign intelligence capability.

*—**David R. Shedd** is a Visiting Distinguished Fellow in the Kathryn and Shelby Cullom Davis Institute for National Security and Foreign Policy, **Paul Rosenzweig** is a Visiting Fellow in the Douglas and Sarah Allison Center for Foreign Policy, of the Davis Institute, and **Charles D. Stimson** is Manager of the National Security Law Program and Senior Legal Fellow in the Center for National Defense, of the Davis Institute, at The Heritage Foundation.*

37. Michael Hayden, "An American Strategy for the Internet and Cybersecurity," Real Clear Defense, October 26, 2015, http://www.realcleardefense.com/articles/2015/10/26/an_american_strategy_for_the_internet_and_cybersecurity_108615.html (accessed April 27, 2016).