A HOOVER INSTITUTION ESSAY

In Defense of FAA Section 702

AN EXAMINATION OF ITS JUSTIFICATION, OPERATIONAL EMPLOYMENT, AND LEGAL UNDERPINNINGS

CHRIS INGLIS AND JEFF KOSSEFF

Aegis Paper Series No. 1604

Executive Summary

The tension between a nation-state's need to detect and interdict threats to life, safety, and property inevitably conflict with the privacy interests of its individual citizens and private sector entities. Increased flattening and convergence of global communications will continue to exacerbate this tension, as nation-states seek to pursue these twin goods within the common spaces shared by protected populations and those who would hold society at risk.

The US Constitution's preamble calls on the government to achieve a common defense while securing the blessings of liberty. The US approach to security achieves both goals by empowering the executive branch to defend the nation while providing the legislative and judicial branches with significant oversight and meaningful involvement. This paper makes the case that the provisions of Section 702 of the FISA Amendments Act are both necessary and appropriate under the US Constitution's mandate that the government pursue all of its aims (i.e., security and *privacy). Moreover, the paper provides compelling evidence to rebut widely circulated myths regarding the actual implementation of Section 702, most notably that NSA exceeded either the intent or the letter of its authorities.*

For this reason, we believe that Congress should reject calls to repeal or amend Section 702. The statute already provides a well-regulated system for intelligence agencies to collect foreign intelligence from non-US persons who are not located in the United States. The National Security Agency has stated that Section 702 is its single most significant tool for identifying terrorist threats.[1] The program is overseen by all three branches of government and has an unprecedented system of checks and balances. In the past seven years, the program has been remarkably effective, both at protecting the privacy of US persons and

Chris Inglis is the Robert and Mary M. Looker Distinguished Visiting Professor for Cyber Studies, United States Naval Academy, and former deputy director of the National Security Agency. Jeff Kosseff is an assistant professor of cybersecurity law at the US Naval Academy. The opinions expressed in this paper are only those of the authors, and do not necessarily reflect the views of the Naval Academy, Department of Navy, or National Security Agency.

at obtaining valuable intelligence from foreign sources. Accordingly, Congress should reauthorize this valuable foreign intelligence program.

Introduction

In early June 2013, the *Guardian* and *Washington Post* newspapers released documents leaked by Edward Snowden, purporting to disclose surveillance by the National Security Agency (NSA), that were to inflame the imaginations of millions of people around the globe. Many of the disclosures by Snowden related to the Foreign Intelligence Surveillance Act's (FISA) Section 702 (often referred to by the term PRISM).

The vast majority of Americans knew little or nothing of the inner workings of the FISA (first passed in 1978 and amended in 2008). In the days and weeks following publication of Snowden's allegations, significant attention was given in both press accounts and congressional hearings to alleged misuse of the capability in apparent violation of the authorities conveyed by FISA and controls that had been constructed to constrain the government's actions. Indeed, just a few weeks after the *Guardian* report, two law professors wrote an op-ed in the *New York Times* in which they boldly branded the NSA programs as "criminal," while in the same paragraph acknowledging that they "may never know all the details of the mass surveillance programs."[2] Allegations that NSA directly targeted the servers of major US telecommunication providers or had violated Section 702's requirement for targeted collection quickly followed—based only the presumption that such abuse could have been tolerated or abetted by the controlling authorities. And that has been precisely the problem with much of the commentary about Section 702: condemnations of the program based on few actual facts and lacking the context of FISA's purpose and the controls designed and implemented across three branches of government to constrain the government's actions to those purposes alone.

In this paper, we seek to advance a simple policy suggestion: Congress should reauthorize this important program without any significant changes to the statute. The critics of Section 702 have not presented a compelling argument—based on how the statute *actually* works—that would compel Congress to make any significant changes to this program. Rather, Section 702 fully meets the Constitution's charge: providing national security *and* individual privacy for all those protected by the Constitution. Put simply, there is no good case for not reauthorizing it when it comes up for renewal next year.

Indeed, the criticisms of Section 702—though often well intentioned—generally arise from widespread misunderstandings of the program's capabilities, controls, and results. There are numerous reasons for this confusion: the complex structure of the

program, the understandable passions provoked by the Snowden disclosures, and the inherently secret nature of classified information, to name a few. As Congress considers reauthorization of this program, we hope that legislators, the press, and the public have a full and complete understanding both of what Section 702 is, and what it is not.

In this paper, we aim to provide the facts that are necessary for a comprehensive and balanced examination of Section 702. A full understanding of government power can never be gained through an examination of a given capability alone. Rather, it is necessary to consider any capability in the context of its purpose (against which criteria should be constructed to gauge its success) and the controls imposed on it (to ensure that the capability is constrained to its intended application). In this manner, *purpose* and *controls* constitute the moral equivalent of bookends that frame and constrain the creation and employment of any government power. This is especially true in the case of government power which must always be framed in light of the constraints embodied in the Constitution, to include the limited purposes for which the government was formed and the explicit constraints upon its authorities characterized in both the articles and the first ten amendments. While less frequently showcased than its counterparts, the Tenth Amendment is perhaps the most significant in this regard: "The powers not delegated to the United States by the Constitution, nor prohibited by it to the States, are reserved to the States respectively, or to the people."[3] Put another way, if a given power is not explicitly granted to the government, it cannot exercise it.

In order to place Section 702 in this context, this paper will explore the three interdependent aspects of the law. What is its purpose (and does that purpose remain true today)? What capability did the law and its attendant implementation bring into being? What are the controls imposed on the use of the authority? After describing the purpose, capability, and controls of Section 702, we examine the program's operational results and consider Fourth Amendment concerns that some critics have raised.

A thorough examination of the purpose, capability, and controls of Section 702 paints a very different picture than the one seen in many critical accounts: the program is a limited and highly effective exercise of the executive branch's constitutional authorities, designed to provide for a common defense while protecting individuals' constitutional liberties. As we explain, there is no evidence of government overreach with Section 702, and a number of statutory safeguards would prevent such hypothetical abuses from occurring in the first place.

Many of the concerns that critics have raised could be addressed by a more frank and open public dialogue about the operations conducted under Section 702. But

the answer, we shall argue, does not lie in changing a law that has served the country remarkably well.

1. Purpose of Section 702

Congress passed Section 702 with a clear purpose: to effect the collection of foreign intelligence in a world that increasingly shares communications infrastructure between legitimate foreign intelligence targets and protected persons when the communications travel through the United States. As we describe in this paper, the law is carefully crafted to achieve the Constitution's twin aims of national security and individual liberties.

While led by the law, this paper will also take care to illuminate the operational case for and use of Section 702. Like the rest of its counterpart sections within the broader Foreign Intelligence Surveillance Act of 2008, Section 702 is wholly focused on the collection and production of foreign intelligence. Moreover, Section 702 only allows the targeting of foreign persons or organizations who are themselves located outside the United States. Given those facts, the question that immediately arises is why this collection is, or should be, allowed to take place within the physical confines of the United States. The answer is straightforward. Collection within the United States, employing US infrastructure and US-based service providers, occasions three particular benefits:

1. The collection activity can be effected with greater care and attendant precision given the relative stability and safety of the domestic environment. In fact, procedures designed under certifications authorized by Section 702 must be constructed to take advantage of this opportunity for greater precision, ensuring that collection is specifically and narrowly focused on legitimate foreign intelligence targets.

2. Given the precision afforded in the selection and capture of the collected materials, Section 702 collection is therefore far more likely than its counterpart Executive Order 12333 collections (which typically take place in uncontrolled environments outside the Unite States) to yield pristine, intact copies of the desired communication transactions. The particular challenge of collecting unintended material adjacent to the targeted communication encountered in 702's upstream collection will be discussed later in the paper and is addressed by imposing controls on its processing and handling.

3. FISA ensures that the collection is authorized and regulated by the combined efforts of three branches of government.

Section 702 laid in place a legal regime unique in the world that involves all three branches of government to authorize, oversee, and regulate collection effected under provisions of 702. This complex set of legal rules, however, has led to great misunderstanding of its initial purpose.

To fully understand the purpose of Section 702, it is helpful to review its history. The current framing of Section 702 is contained in the Foreign Intelligence Surveillance Act Amendments Act of 2008 (often referred to as the FISA Amendments Act or FAA). While sometimes perceived as a means to expand the capabilities of the government in effecting foreign intelligence collection, the FAA was actually designed to sustain capabilities codified in the FISA legislation of 1978, while addressing thirty years of technology modernization which had rendered both the capabilities authorized by FISA and, equally important, the controls imposed on it considerably less effective than when first implemented in the late 1970s. Two particular trends across those years warrant a more careful examination.

The first was 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. And yet all through this period, the provisions of FISA 1978 presumed that the preponderance of communications conveyed by "wire" would be local communications and those transiting "in the air" (e.g., satellite communications in 1978) would be international in nature. As a consequence, the provisions of FISA 1978 tightly regulated NSA's access to wireline communications with considerably less attention given to those transiting in the air. The flaw in the 1978 formulation wasn't that its technology forecast was wrong. It was in trying to codify technology trends at all. FISA 2008 rewrote the 1978 law to sustain its provisions for both national security *and* privacy protections in a technology neutral context.

Second, the explosion of commercial offerings of various technologies enabled tremendous agility on the part of consumers, not only in the services they could employ but in their choice and use of selectors (e-mail address or telephone numbers) across a growing number of services. While this must be perceived for the vast majority of users as an unalloyed good, it 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 approvals. To address the need to equip national intelligence with an agility on par with legitimate

intelligence targets, FISA 2008 replaced the FISA 1978 selector-by-selector-based approvals with a certification approach that created and approved *procedures* to be followed by the executive branch for determining and employing individual selectors in foreign intelligence collections, in lieu of continuing to require selector-by-selector approvals. This compromise resulted in the creation of a requirement for "certifications" under FISA 2008, yielding both agility and accountability for the executive branch's use of the FISA capability.

The Senate Judiciary Committee report 112-229 of September 20, 2012, noted in its introduction to the FAA Sunsets Extension Act of 2012 (which extends FAA 2008 for another three years) that:

> . . . as amended, [this bill] reauthorizes Title VII of FISA for three years, enabling continued use of these important surveillance tools, while improving and clarifying the oversight and accountability provisions in Title VII to help ensure adequate protection of the privacy rights and civil liberties of persons in the United States.[4]

Indeed, Congress carefully crafted Section 702 to establish an effective, but narrow, system that focuses on the acquisition of foreign intelligence information from non-US persons *outside* of the United States. Congress's intentions are clear both from the plain text of the statute and from the legislative history.

Even the title of Section 702—"Procedures for targeting certain persons outside the United States other than United States persons"—indicates that Section 702 is not intended to gather information about US citizens.[5] The statute then makes clear that collection only is authorized if the targets are reasonably believed to be non-US persons located outside of the United States, and it imposes extensive limits on the collection and use of the data (described in more detail in Part 2 of this paper). The statute also requires intricate 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."[6]

Quite simply, there are few US law enforcement regimes that are subject to such a rigid set of detailed statutory and regulatory requirements. The plain language of the statute evinces Congress's clear intent to create a program that efficiently and effectively gathers foreign intelligence information, while avoiding, to the greatest extent possible, targeting the content of communications that involve US citizens or individuals reasonably believed to be located in the United States.

Section 702's legislative history also demonstrates the narrow purpose of the program. In its report accompanying an earlier version of the FAA, the Senate Intelligence Committee wrote that its goal "has been to develop a sound legal framework for essential intelligence activities in a manner consistent with the U.S. Constitution."

Congress also has recognized the vital and irreplaceable national security functions of Section 702. In the House report recommending the 2012 reauthorization of FAA, legislators wrote that Section 702 information "is often unique, unavailable from any other source, and regularly provides critically important insights and operationally actionable intelligence on terrorists and foreign intelligence targets around the world."[7]

Despite the clear intent of Section 702 as a means of gathering foreign intelligence information on targets who are non-US persons located outside of the United States, critics are worried about the incidental interception of the communications of US persons. They raise the valid—though unsupported—concern that Section 702 is intended to be a back door around the general Fourth Amendment requirement that the government obtain a warrant before collecting the communications of US persons.[8] This argument fails to appreciate the reason that Section 702 must allow the possibility of incidental interception: it is impossible for the government, before beginning a surveillance operation, to know with certainty the identities of every individual with whom the target might communicate. As one federal court recognized in 2000, the government "is often not in a position of omniscience regarding who or what a particular surveillance will record."[9] Any incidental collection of a US person's communications is just that: incidental. To be clear, because any single communication is associated with two or more parties (a sender and one or more recipients), the "incidental communication" described here is one and the same as the communication that has been legitimately targeted and collected by the government (otherwise the legal phrasing applied to the communication would be an "unintended collection," a subject which must not be conflated here). It is certainly possible that all parties to a given communication are legitimate targets of surveillance. But in every other case, all parties not explicitly targeted by the government will be considered as incidental to the intended collection. In this manner, an absolute prohibition on incidental collection would effectively shut down our ability to collect foreign intelligence in any case where the status of all parties in a given communication is unknown.

Critics also argue that Section 702 is merely the intelligence community's attempt to avoid seeking Foreign Intelligence Surveillance Court approval of an order, supported by probable cause, under Title I of FISA.[10] This argument ignores the fact that Title I is used in part to collect foreign intelligence from targets who are US persons or located in the United States, and therefore are entitled to the full panoply

of rights under the US Constitution. It would be unprecedented—and impractical—to require intelligence analysts to obtain a search warrant every time that they sought to gather information regarding a target who is neither a US person nor located in the United States. As the Public Civil Liberties Oversight Board (PCLOB) aptly concluded in its 2013 report, Section 702 "enables a much greater degree of flexibility, allowing the government to quickly begin monitoring new targets and communications facilities without the delay occasioned by the requirement to secure approval from the FISA court for each targeting decision."[11] This flexibility allows the government to more quickly learn of a terrorist plot or other national security threat that it otherwise would not have learned of if it had to comply with the full court procedures.

As we show in the next section, the program is structured to provide the government only with the capabilities to conduct these foreign intelligence operations, targeting non-US persons who are located outside of the United States.

2. Capability of Section 702

In this section, we describe the actual capability of the Section 702 program, both as stated in the law and as implemented by the NSA.[12] NSA's actual surveillance capabilities under Section 702 are far narrower than many media reports would suggest.

Contrary to incomplete and inaccurate reporting shortly after the Snowden leaks, Section 702 does not provide NSA or other governments with the ability to "tap into" service providers' US servers. On June 6, 2013, the *Washington Post* reported that the NSA and FBI "are tapping directly into the central servers of nine leading US 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."[13] Professor Peter Swire, who served on the President's Review Group on Intelligence and Communications Technology, recently released a comprehensive paper that debunks that myth. He concludes that "the government does not have direct access under the PRISM program, but instead serves legal process on the providers similar to other stored records requests."[14]

Section 702 focuses on ensuring that the surveillance is conducted for foreign intelligence purposes and targets non-US persons. To wit, the first two subparts of Section 702 impose a number of limitations on the collection of foreign intelligence information under the program:

- Both the attorney general and director of national intelligence must authorize any collection.[15]

- The collection can be authorized for no more than one year.[16]

- Section 702 operations "may not intentionally target any person known at the time of acquisition to be located in the United States."[17]

- Even if the individual is reasonably believed to be located outside of the United States, the agencies cannot target that person with the ultimate purpose of targeting a person reasonably believed to be located within the United States (a prohibition against so-called "reverse targeting").[18]

- Agencies may not target a US person (such as a US citizen or permanent resident), even if that person is reasonably believed to be located outside of the United States.[19] While targeting US person communications outside the United States was previously permitted by FISA 1978 under attorney general authorization, the FAA of 2008 significantly strengthened protections given to US persons by requiring that a probable-cause warrant be obtained for *any* collection targeting the content of a US person's communications, regardless of the person's location in the world.

- Even if the target is a non-US person located outside of the United States, the agencies may not "intentionally acquire communication for which the sender and all intended recipients are known at the time of the acquisition to be located inside of the United States."[20]

- The program must be conducted "consistent" with the Fourth Amendment.[21]

The entire operating structure of Section 702 is designed to satisfy these restrictions. It is important to note that the burdens imposed by these restrictions are never relieved—from the collection and processing of communications, through analysis and reporting, to dissemination and retention. To fully understand the operations of the program, it is useful to consider the process in five stages:

1. **Certification:** receiving approval from the Foreign Intelligence Surveillance Court for collecting intelligence for a foreign intelligence purpose.

2. **Targeting:** identifying targets who are non-US persons located outside of the United States and the e-mail addresses, phone numbers, and other communications facilities associated with them (known as "selectors").

3. **Tasking:** obtaining the communications from selectors that are used by these targets.

4. **Analysis:** querying the raw data and disseminating intelligence.

5. **Retention and destruction:** ensuring that NSA does not indefinitely hold on to all raw data after tasking.

A. Certification

The attorney general and director of national intelligence annually certify to the Foreign Intelligence Surveillance Court a list of foreign intelligence topics for which intelligence agencies seek to collect information under Section 702.[22] The certifications must attest that "a significant purpose of the acquisition is to obtain foreign intelligence information" and describe, in detail, the procedures that ensure that US persons are not targeted.[23] Although the complete list of such topics is classified, the certifications are formally documented by the executive branch and must be approved by the judicial branch (i.e., the Foreign Intelligence Surveillance Court). Moreover, government officials have publicly stated that the topics include international terrorism and acquisition of weapons of mass destruction.[24]

The Foreign Intelligence Surveillance Court's role is to review certifications, request amendments, and determine whether the targeting procedures are reasonably designed to ensure that actions are "limited to targeting persons reasonably believed to be located outside the United States."[25]

B. Targeting

If an NSA analyst identifies a non-US person located outside of the United States as a potential target for gathering foreign intelligence for a purpose that the Foreign Intelligence Surveillance Court has certified, the analyst must follow a detailed, and FISC-approved, set of targeting procedures.

First, the analyst must determine the specific e-mail address, telephone number, or other communications facility that is used by the target (known as a "selector.").[26] The NSA analyst then checks multiple sources to verify both the "foreignness" of the target and the connection between the target and the selector.[27]

After an extensive review of the NSA's targeting procedures, the Privacy and Civil Liberties Oversight Board agreed that this foreignness determination is "not a 51% to 49% test," and that if there is "conflicting information indicating whether a target is located in the United States or is a U.S. person, that conflict must be resolved" and the user must be determined to be a non-US person reasonably believed to be located outside the United States prior to targeting.[28] This procedure is highly effective; in 2013, the Justice Department conducted a comprehensive review of one year of data regarding NSA's targeting decisions and concluded 99.6 percent of the selectors that

NSA tasked under Section 702 did not have any users who were located in the United States or were US persons.[29]

The NSA analyst also must document the specific foreign intelligence purpose for which it seeks to target an individual.[30] The analyst must specifically document the foreign power or foreign territory about which this surveillance will provide foreign intelligence.[31] NSA analysts also typically include a brief statement that "further explains the analyst's rationale for assessing that tasking the selector in question will result in the acquisition of the types of foreign intelligence information authorized by the Section 702 certifications."[32]

Upon completion of the due diligence, the analyst provides documentation of this verification to two senior NSA analysts. Only after the senior analysts approve the request may a service provider be compelled to provide the communications associated with the selector through tasking.

C. Tasking

When a selector is tasked, the NSA receives information from service providers through one of two processes.

The first process, referred to in the press as the PRISM program, requires service providers to provide NSA with communications to or from the explicitly tasked selectors. Before this data is made available to NSA analysts, it is reviewed by service provider technicians to ensure that the communications are restricted to only the types of communications that are the subject of the government's request. This provides yet another additional limit on distribution under the program. According to data that the government provided to the Foreign Intelligence Surveillance Court, more than 90 percent of NSA's Section 702 data came from this process.

The second process, known as upstream collection, has received the most public scrutiny and is often conflated with PRISM, though it accounts for approximately 10 percent of all Section 702 data. In the upstream process, the NSA works with telecommunications providers to obtain telephone and Internet communications that traverse US communications infrastructure.[33] The operational motivation of this capability is not intended to duplicate collections available from PRISM. Rather, it is designed to acquire targeted "in-stream" communications not under the direct control of the service providers. As with the PRISM process, electronic communications collected via the upstream process can be to or from a tasked selector. Unlike communications collected via PRISM, upstream communications also can be "about" a selector.[34]

An "about" communication "is one in which the tasked selector is referenced within the acquired Internet transaction, but the target is not necessarily a participant in the communication."[35] For instance, if the selector is a target's e-mail address, the NSA could acquire e-mail messages that contain that address in the body of the e-mail, regardless of whether the sender or recipient is a target.[36]

NSA collects two types of Internet communications transactions through the upstream process: single communication transactions (SCTs) and multi-communication transactions (MCTs). SCTs, which comprised about 90 percent of the upstream communications that the NSA collected during a six-month sample period in 2011,[37] are discrete communications, such as a single e-mail message.[38] MCTs, in contrast, consist of multiple communications that are packaged and transmitted as a single entity (i.e., the inbox listing of a single communicant is often transmitted by service providers as a single intact stream of bits, even though it represents the leading edge of many individual e-mails).[39] Due to this fact, and the ever-changing nature of service providers' protocols and other technology, it is not always technically possible for the government to collect only the portions of MCTs that are foreign communications to, from, or about the tasked selectors. If the NSA identifies a communication within an MCT as being to, from, or about a selector, the NSA obtains the complete MCT. Accordingly, there are instances in which a discrete communication within an MCT contains a discrete domestic communication that is not to, from, or about a tasked selector.[40]

Critics of Section 702 claim that the "about" process, when combined with the collection of discrete messages in an MCT, results in the collection of purely domestic communications, or communications that contain US person information and are not to, from, or about a tasked account.[41] To be sure, such collection does occur, but it represents a tiny sliver of the total upstream data. A Foreign Intelligence Surveillance Court review of a sample provided by NSA found that such incidental collection only occurs for approximately 0.02 percent of upstream communications.[42] Moreover, upstream data accounts for less than 10 percent of all communications collected under Section 702.[43]

Even so, recognizing the possibility that MCTs might contain US person data, the FISC has imposed additional procedures to ensure due diligence in detecting their presence and effecting appropriate protections. Once the data are acquired, NSA analysts must review a sample of the communications to ensure that they are related to the target and foreign intelligence purpose that the analyst initially identified. The analyst also must review the sample to ensure that the target is a non-US person located outside of the United States.[44] Selectors that do not meet this criteria are "de-tasked" and not available for analysis.[45]

Moreover, NSA's minimization procedures require the agency to acquire information in a manner that is designed "to the greatest extent reasonably feasible, to minimize the acquisition of information not relevant to the authorized purpose of the acquisition."[46]

The minimization procedures also take care to account for the change of a target's location from outside of the United States to inside the United States. Even if the target is a non-US person, the NSA will cease Section 702 operations directed at that target if it reasonably believes that the target is now located in the United States. For instance, suppose that an NSA analyst uses Section 702 to lawfully obtain the e-mails of a suspected terrorist who is located in Syria. If the analyst learns that the target has since moved to New York, the acquisition "will be terminated without delay."[47] Domestic surveillance laws, under the purview of the FBI, would apply at that point.

D. Analysis

Once NSA has properly tasked selectors and obtained information from communications, it faces a series of limits on its ability to analyze this data.[48] It is important to recognize that the following restrictions are applied to *collected* communications—specifically, those communications that have already shown themselves to be responsive to a foreign intelligence query. Put another way, the mere fact that a given communication contains a selector of legitimate interest to an NSA intelligence analyst does not relieve the burden imposed by FAA 2008 to proactively sustain protections for US persons throughout the collection-to-dissemination process.

Among the most prominent criticisms of Section 702 is that analysts could query raw communications to obtain information about US persons.[49] ("Raw" means that, while each communication has already been shown to contain a targeted selector, it has not yet been reviewed to determine its actual relevance or import to the given foreign intelligence inquiry.) In other words, critics argue, this would be a back door for spying on US persons without a warrant.[50]

NSA's minimization procedures, however, explicitly prevent such intentional backdoor surveillance. Analysts may only search for terms, such as phone numbers or key words, that are "reasonably likely to return foreign intelligence information."[51] As an absolute rule, however, analysts may not use an identifier of an identifiable US person to search upstream Internet communications.[52] Moreover, NSA analysts generally are prohibited from using a US person's identifier as a search term for other Section 702 data unless they justify the specific search in a *written* statement of facts and receive additional approval *before* conducting the query.[53] According to PCLOB, 198 US person identifiers were approved for NSA queries in all of 2013.[54]

Moreover, it is important to note that the restrictions on NSA use of US person terms apply to the use of any US person term, regardless of the context. For example, an analyst pursuing a possible terrorist threat to an airline incorporated in the United States would need to follow the procedures described above before searching already collected terrorist communications for the presence of any of the following terms: "American Airlines," "United Airlines," or a named US person or corporation assessed to be a *target* of a given terrorist plot.

NSA analysts also are prohibited from using broad, overly generic search terms or conducting other similar unrestricted fishing expeditions.

The minimization procedures also recognize the legitimate concerns that MCTs may contain wholly domestic, discrete communications that are not to, from, or about the tasked selectors. The procedures require NSA to take "reasonable steps" to use technical means to segregate MCTs for which the active user—i.e., the sender or recipient—is "reasonably believed" to be located within the United States.[55] The NSA also will segregate MCTs if the active user's location cannot be determined. Those segregated MCTs are then reviewed by NSA analysts, who determine whether the transactions contain domestic communications.[56] The analysts are required to document all of these determinations.

If an individual communication within an MCT is not to, from, or about a tasked selector and is to or from a US person or an individual "reasonably believed" to be in the United States, that individual communication *cannot* be used, except "to protect against an immediate threat to human life[.]"[57] If the NSA uses the information for this purpose, it must report the use to the director of national intelligence and the Justice Department, which informs the Foreign Intelligence Surveillance Court.[58]

The NSA also has imposed strict limits on its ability to share information that it has obtained under Section 702. The minimization procedures state that NSA may only disseminate data of or concerning a US person under one of a handful of limited conditions, such as the individual being an agent of a foreign power.[59] Even when the NSA is authorized to disseminate this data, it usually masks the US person's identity and redacts other identifying details.[60]

E. Retention and Destruction

Section 702 has been portrayed in some accounts as the government's attempts to stockpile massive amounts of communications, including some involving US citizens. To be sure, Section 702, like other intelligence operations, involves vast volumes of e-mails and other communications. However, the minimization procedures prevent

NSA from holding on to these communications indefinitely, particularly if the communications are domestic.

If the NSA determines that a communication is purely domestic, the communication must be "promptly destroyed upon recognition" unless the NSA director makes the specific determination that the sender or recipient has been lawfully targeted and that the communication is reasonably believed to contain significant foreign intelligence information, evidence of a committed or planned crime, or technical information for signal exploitation or related purposes.[61] The agency also may retain communications that contain information indicating an imminent threat of serious harm to life or property.[62]

The NSA's minimization procedures require all telephone and Internet transactions that the agency obtained from service providers to be destroyed within five years of the FISC certification, "unless NSA specifically determines" (1) that retention is "necessary for the maintenance of technical data bases;"(2) that the data is evidence of a past, ongoing, or future crime and has been turned over to federal law enforcement; or (3) the NSA satisfies the dissemination standards described in the previous section.[63] Moreover, all upstream Internet transactions must be destroyed within two years of the expiration of the FISC's certification, unless at least one communication within the transaction meets the NSA's retention standards and is to, from, or about a tasked selector, a non-US person, or a person not located in the United States.[64] This procedure prevents the NSA from stockpiling decades of raw data regardless of relevance.

3. Controls on Section 702

Much of the criticism of Section 702 has been premised on the assumption that a rogue NSA agent could have sweeping and unregulated access to the communications content, using the program to spy on personal enemies and commit other serious privacy violations. As with many of the criticisms surrounding Section 702, this arises largely from a misunderstanding of the complex structure of the program. An objective examination of Section 702's intertwined network of checks and balances paints an entirely different picture. The Section 702 program has extensive oversight by the NSA, other executive branch agencies, the judicial system, and Congress.

An NSA analyst would be ill-advised to abuse the Section 702 system, particularly to gather data on a US person without proper authority. Such a move could be reviewed by numerous superiors at the NSA, the Justice Department, the Office of the Director of National Intelligence, the Inspectors General of the NSA and other agencies, four congressional committees, and the Foreign Intelligence Surveillance Court. In no case could the action be taken unilaterally without the material involvement of one

or more of the above named parties. Accordingly, it is unsurprising that the criticism of Section 702 has focused on *hypothetical* rather than *actual* abuses of Section 702 authorities; the system of safeguards across all three branches of government is carefully designed to prevent misuse of the data.

A. NSA

As discussed throughout Part 2 of this paper, analysts must produce extensive documentation of their decisions regarding targeting, tasking, querying, and retention of communications. The controls are particularly stringent when the communications may be to, from, or about a US person or person located in the United States. NSA's Signals Intelligence Directorate regularly audits a sample of queries that include US person identifiers. This provides an additional check to ensure that analysts are not misusing the data.

NSA requires analysts to enroll in an extensive training curriculum before allowing them to access Section 702 data or other signals intelligence information.[65] Although many of the training modules are classified, the American Civil Liberties Union obtained unclassified versions of some of the training materials via the Freedom of Information Act. A review of these materials demonstrates that the NSA not only explains the law, but also provides practical guidance as to how analysts can meet those legal requirements. For instance, the following are the NSA's training instructions in the case of inadvertent collection of US person information:

- Stop collection immediately!
- Cancel reports based on that collect.
- Notify your supervisor or auditor.
- Write up an incident report immediately.
- Submit the incident write-up for inclusion in your organization's IG [inspector general] Quarterly input.[66]

If NSA employees fail to follow any of the detailed limitations on their ability to collect or use the Section 702 data, they are subject to a number of internal compliance positions, including the employees' supervisors, NSA's director of civil liberties and privacy, NSA's general counsel, and NSA's inspector general. And while concerns about potential abuse properly inform the diligence with which controls are designed and enforced, numerous and extensive investigations conducted by outside parties before and after the sensational claims of Edward Snowden in 2013 have yet

to document a single case of abuse of Section 702 data by an individual or a systemic abuse by the NSA. Indeed, as Geoffrey Stone, the Edward H. Levi Distinguished Service Professor of Law at the University of Chicago and a member of the President's 2013 NSA Review Group, stated in an op-ed in March 2014:

> From the outset, I approached my responsibilities as a member of the Review Group with great skepticism about the NSA. I am a long-time civil libertarian, a member of the National Advisory Council of the ACLU, and a former Chair of the Board of the American Constitution Society. To say I was skeptical about the NSA is, in truth, an understatement. I came away from my work on the Review Group with a view of the NSA that I found quite surprising. Not only did I find that the NSA had helped to thwart numerous terrorist plots against the United States and its allies in the years since 9/11, but I also found that it is an organization that operates with a high degree of integrity and a deep commitment to the rule of law.
>
> Like any organization dealing with extremely complex issues, the NSA on occasion made mistakes in the implementation of its authorities, but it invariably reported those mistakes upon discovering them and worked conscientiously to correct its errors. The Review Group found no evidence that the NSA had knowingly or intentionally engaged in unlawful or unauthorized activity. To the contrary, it has put in place carefully-crafted internal procedures to ensure that it operates within the bounds of its lawful authority.[67]

B. Other Executive Branch Agencies

NSA's Section 702 program also is subject to oversight by a number of other executive branch agencies, reducing the likelihood of a single department head allowing compliance to slip through the cracks.

Every other month, both the Justice Department and Office of the Director of National Intelligence review NSA analysts' documentation of its compliance with Section 702 restrictions. Both agencies review large samples of both the tasking documentation and the report that NSA has disseminated; Justice Department attorneys determine whether the documentation meets the statutory and procedural requirements.[68]

The Justice Department and Office of the Director of National Intelligence receive reports of suspected noncompliance with Section 702 procedures, investigate incidents, and regularly discuss compliance issues with intelligence agencies.[69] Separately, the inspectors general of other intelligence and law enforcement agencies also have the legal authority to review the NSA's Section 702 programs.[70]

C. Congress

The Justice Department and the Office of the Director of National Intelligence provide the results of their routine reviews of targeting and minimization to the House and Senate Judiciary and Intelligence committees.[71] The agencies also are required to report any compliance incidents to congressional committees in a semiannual report.[72]

FISA requires the report to contain extensive details—many of which are classified—to ensure that members of the four committees have a complete understanding of the Section 702 programs. Among the required components of the semiannual report are the Foreign Intelligence Surveillance Court's certifications, any compliance reviews conducted by the Justice Department or Office of the Director of National Intelligence, and descriptions of all incidents of noncompliance.[73] The committees also hold hearings on the program.[74]

D. Judiciary

Section 702's operations are subject to extensive oversight by the Foreign Intelligence Surveillance Court (FISC). Although the court's independence and transparency have been derided by critics, they ignore the fact that the court is comprised entirely of Article III, life-tenured judges who are appointed by the president and confirmed by the Senate. These are the same judges who hear the full range of civil and criminal cases over which our federal courts have jurisdiction.

As discussed in Part 2 of this paper, FISC must review and approve the Section 702 certifications *and* minimization procedures, ensuring that the intelligence community only operates the Section 702 program for purposes authorized by law. Moreover, FISC receives all of the reports of noncompliance, the Justice Department/director of national intelligence semiannual reports, annual Section 702 reports produced by each intelligence agency, and inspector general reports about Section 702.[75]

Courts do more than comment on the Section 702 programs; they work with the agencies to change procedures that they do not believe satisfy the program's statutory or constitutional mission. Consider Judge John Bates's 2011 opinion, in which he considered the incidental collection of wholly domestic communications within MCTs.

In May 2011, the government filed a letter with the court, clarifying that MCTs may contain discrete communications that are not to, from, or about the tasked facility.[76] Judge Bates, concluding that these acquisitions "exceeded the scope of collection previously disclosed by the government, and approved by the Court," quickly ordered

briefings and a hearing on the issue.[77] After a thorough review of the evidence, Judge Bates concluded that this acquisition complies both with the statutory requirements of Section 702 and with the Fourth Amendment.

However, Judge Bates stated that "NSA could do substantially more to minimize the retention of information concerning United States persons that is unrelated to the foreign intelligence purpose of its upstream collection."[78] Judge Bates then listed a number of additional limits the government could impose, including restricting access to upstream communications to a smaller subset of trained analysts and requiring analysts to analyze discrete communications for compliance with Section 702. Judge Bates noted that some of the steps that he suggested might be impracticable, but that "by not fully exploring such options, the government has failed to demonstrate that it has struck a reasonable balance between its foreign intelligence needs and the requirement that information concerning United States persons be protected."[79]

After this opinion, the NSA revised its minimization procedures to prohibit its analysts from using discrete communications from within an MCT unless the analyst first has reviewed that specific communication to determine whether it is to or from a non-US person who is located out of the United States. If not, then the analyst may only use that communication to protect against immediate threats to life.[80]

Judge Bates's opinion demonstrates Section 702's system of effective checks and balances in action. Step back to think about the efficiency of these oversight mechanisms: in May, the government voluntarily reported new information about the program's operations to the court; in October, the court issued an extensive examination of the program's legal underpinnings and areas for improvement; and, by the end of the year, the government had incorporated that feedback into its operations. As intelligence officials noted in congressional testimony later that year, the court's "exhaustive analysis of the Government's submission, like its other decisions, refutes any argument that the court is a 'rubber stamp,' and demonstrates the rigorous nature of the oversight it conducts."[81]

4. Results of Section 702

To fully assess a government program, it is necessary to consider not only its purpose, capability, and controls, but also the benefits that it brings to the general public. In the case of Section 702, that benefit is increased national security. Unfortunately, due to the necessarily classified nature of our national security operations, it is difficult to describe many of the specific instances in which Section 702 data has helped to protect Americans. However, the publicly reported aggregate information demonstrates the powerful and irreplaceable role that Section 702 plays in our

national security and intelligence operations. President Obama stated that after he "looked through specifically what was being done," he determined that sections 215 and 702 "offered valuable intelligence that helps us protect the American people and they're worth preserving."[82]

After its thorough review of Section 702, the independent civil liberties oversight board concluded that the statute "has enabled the U.S. government to monitor these terrorist networks in order to learn how they operate and to understand how their priorities, strategies, and tactics continue to evolve,"[83] noting that more than a quarter of the NSA's reports involving international terrorism are based at least partly on Section 702 data.

For instance, the oversight board cited the case of Khalid Ouazzani, who was located in Missouri and was part of a plan to bomb the New York Stock Exchange. The NSA learned of him during its surveillance of a Yemeni extremist's e-mail address.[84] He was apprehended and later convicted after the NSA conveyed this intelligence to the FBI.[85] He also was a cooperating witness for the prosecution of two Al Qaeda supporters.[86]

Similarly, the oversight board cited NSA's surveillance of the e-mail address of an Al Qaeda courier in Pakistan that led the agency to Najibullah Zazi, a Denver man whom the courier contacted for information about bomb-making.[87] The NSA provided this tip to the FBI, which tracked Zazi as he and collaborators drove to New York to detonate explosives on subways. Zazi learned that he was being tracked, returned to Colorado, and was soon arrested. As the oversight board correctly concluded, without the initial Section 702 information, obtained through monitoring a Pakistani, "the subway-bombing plot might have succeeded."[88]

Section 702 information also contributed to the arrest in Chicago of David Coleman Headley, who had planned to attack a Danish newspaper that had printed cartoons of the Prophet Muhammad.[89] Headley also had helped to plan the 2008 terrorist attacks in Mumbai and was sentenced to thirty-five years in prison.[90]

An expert intelligence review group, appointed by the president, concluded in 2013 that Section 702 "has clearly served an important function in helping the United States to uncover and prevent terrorist attacks both in the United States and around the world."[91] The record of Section 702 in supporting the collective security of nations other than the United States is particularly notable. Government officials frequently testified in open congressional session during the summer of 2013 that Section 702 had played an instrumental role in the disruption of at least fifty-four terrorist plots around the world between 2001 and 2013. Forty-one of these were described as having a nexus in a country other than the United States, of which twenty-five were

plots that were to take place in Europe. In each of these cases, information derived from Section 702 was shared by the United States with counterparts in countries believed to be under threat, leading to the application of appropriate instruments of national and international (collective) power by those nations under a rule of law consistent with both the United States and the local jurisdiction. In this manner, Section 702 contributed to the collective security of many nations under a scheme that ensured a rule of law defined by the *highest* common denominator between national approaches, not the lowest.

5. Constitutionality of Section 702

Since Section 702's enactment—and especially since the 2013 Snowden disclosures—critics have asserted that the program violates the Fourth Amendment's prohibition on unreasonable searches and seizures.[92] However, courts have repeatedly held that Section 702—as written and implemented—complies with the Fourth Amendment.[93] The courts' Fourth Amendment reasoning demonstrates that Section 702 not only is constitutional, but is sound public policy that protects both national security and individual liberties. In other words, for the same reasons that Section 702 is constitutional (i.e., its minimal intrusion of privacy interests in comparison to the significant security benefits), it also is sound public policy, and Congress should reauthorize the statute without any significant revisions.

The Fourth Amendment states:

> The right of the people to be secure in their persons, houses, papers, and effects, against *unreasonable* searches and seizures, shall not be violated, and *no Warrants shall* issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.[94]

At the outset, the Fourth Amendment's protections do not "apply to activities of the United States directed against aliens in foreign territory."[95] Accordingly, the Fourth Amendment concerns surround the incidental collection of *US persons'* communications.

Thus, in assessing Section 702's compliance with the Fourth Amendment, we must examine: (1) whether a warrant is required for the incidental collection of the communications of US persons; and (2) whether the process is reasonable.

A. Warrant Requirement

The Fourth Amendment's warrant requirement does not apply to Section 702 for two reasons.

First, courts have long held that "incidental collections occurring as a result of constitutionally permissible acquisitions do not render those acquisitions unlawful."[96] Section 702 is directed at intelligence from non-US persons who are located outside of the United States. Any incidental collection of US persons' information, therefore, is not subject to the Fourth Amendment warrant requirement.

Second, Section 702 falls within the foreign intelligence exception to the warrant requirement. The Supreme Court has long recognized that the warrant requirement does not apply "when special needs, beyond the normal need for law enforcement, makes the warrant and probable-cause requirement impracticable."[97] Although the Supreme Court has not addressed whether foreign intelligence is a "special need" that is exempt from the warrant requirement, several other courts have held that it is. For instance, the Foreign Intelligence Surveillance Court of Review held that the special needs exception applies to foreign intelligence because the purpose "goes well beyond any garden-variety law enforcement objective."[98] The Foreign Intelligence Surveillance Court held that this exception applies even to the acquisition of MCTs that may contain communications of or concerning US persons.[99] In a criminal case, a federal judge rejected the defendant's argument that obtaining information about him through Section 702 violated the warrant clause, concluding that there "is no reasonable argument the government's need for the acquisitions is merely routine law enforcement."[100] In short, courts have repeatedly held that Section 702 is exempt from the warrant requirement under the special needs exception.

B. Reasonableness

Even when a warrant is not required, the Fourth Amendment protects US persons from searches and seizures that are "unreasonable."[101] To determine the reasonableness of a search, courts consider the "totality of the circumstances," in which they balance "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 governmental interests."[102] Applying this balancing test to Section 702, the government interests in national security outweigh the privacy intrusions, when considered in light of the numerous privacy safeguards that are at the core of Section 702.

To be sure, Section 702 does implicate individual privacy due to the collection of some US persons' communications. However, it is important to remember that this collection is only *incidental,* and that the Fourth Amendment does not apply to the collection of communications of non-US persons located outside of the United States.

For that small subset of information that falls within Fourth Amendment protections, the NSA and other agencies are subject to extensive restrictions on the collection,

use, and retention of the data, as described in Part 2 of this paper. In a 2014 order affirming the constitutionality of Section 702, the Foreign Intelligence Surveillance Court concluded that the combined effect of the targeting and minimization procedures "has been to substantially reduce the risk that non-target information concerning United States persons or persons inside the United States will be used or disseminated and to ensure that non-target information that is subject to protection under FISA or the Fourth Amendment is not retained any longer than is reasonably necessary."[103]

On the other side of the reasonableness equation, the government has a strong interest in using Section 702 to meet its national security goals. The NSA has 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."[104] Indeed, the Supreme Court has held that it is "obvious and unarguable that no governmental interest is more compelling than the security of the Nation."[105] Section 702 does not merely provide marginal or hypothetical national security protections; it is *the most* essential tool that the NSA has in its arsenal. Therefore, the governmental interest is quite strong.

Gathering national security information is particularly difficult when dealing with diffuse foreign terrorist groups such as Al Qaeda and ISIS (the Islamic State). The locations, identities, and tools of the foreign targets are constantly changing, requiring intelligence agencies to be agile in their collection and analysis. In its conclusion that the core Section 702 program is constitutional, the Public Civil Liberties Oversight Board reasoned that "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 States."[106]

Critics challenge not only the incidental collection of US person communications, but the subsequent *use* of this raw data by intelligence agencies. In other words, they argue, the Fourth Amendment violation occurs not only upon collection, but also when the NSA and other agencies query the data. A federal judge in Colorado recently rejected this argument, correctly concluding that accessing data that was legitimately collected does not implicate the Fourth Amendment. For instance, the court reasoned, evidence "obtained legally by one police agency may be shared with similar agencies without the need for obtaining a warrant, even if sought to be used for an entirely different purpose."[107] The concerns about such backdoor searches are understandable, but an objective review of the numerous restrictions and controls on tasking can only conclude that it would be not only illegal but impossible for NSA analysts to routinely use Section 702 as a mechanism to avoid the warrant requirement for searches of US persons' communications.

Similarly misguided are challenges to the constitutionality of the upstream collection process. In *Jewel v. NSA,*[108] civil plaintiffs allege that upstream collection is an "illegal and unconstitutional program of dragnet surveillance" and that the government has acquired communications "of practically every American who uses the phone system or the Internet . . . in an unprecedented suspicionless general search through the nation's communications networks."[109] Such concerns are misplaced for two primary reasons. Even if the upstream process were to be considered a "seizure" that is subject to the Fourth Amendment, it clearly is reasonable. As Swire concluded, the upstream process is quite limited and targeted, and "there is a strong basis for rejecting the conclusion that Upstream is 'mass surveillance,' given its much smaller scale."[110] On the other side of the reasonableness equation, the upstream program provides the government with valuable intelligence. For instance, the Senate Select Committee on Intelligence concluded in 2012 that FAA authorities "have greatly increased the government's ability to collect information and act quickly against foreign intelligence targets."[111]

In sum, Section 702 is crucial for intelligence agencies to gather information about ever-evolving terrorist threats. The statute contains strong privacy protections, subject to checks and balances by all three branches of government, to minimize the harm to privacy of US persons. Accordingly, courts correctly determined that, on balance, Section 702 is reasonable and therefore does not violate the Fourth Amendment.

Conclusion

The debate about Section 702 likely will escalate this year as Congress considers reauthorization of the FAA. Such discussion is healthy and necessary for our democratic process. This paper is intended to help inform that debate by describing how Section 702 works in practice. A complete examination of Section 702 reveals a program that is painstakingly designed to protect the privacy of US persons to the greatest extent possible while also gathering valuable intelligence for national security. Section 702 achieves the twin goals of the Constitution's preamble: providing for the common defense and securing the blessings of liberty. And as noted in an extensive 2013 analysis, the United States is the only nation in the world where ". . . such surveillance is subject to review by courts presided over by federal judges, with appeals possible to the US Supreme Court. The law enforcement agencies tasked with complying with FISA are required to provide regular compliance reports to the Congressional committees with responsibility over national security."[112] Given the Constitution's mandate for limited but effective government, this burden is both appropriate and well imposed. It remains the gold standard in a world searching for the means to achieve the dual aims of security and the defense of individual liberties. The critics of Section 702 have failed to provide persuasive evidence that Section 702 is either unconstitutional or bad public policy, and therefore have not

made the case for modification or repeal of the law. For that reason, Congress should reauthorize Section 702 without any significant amendments.

The biggest failure surrounding Section 702 has been the lack of clear information for the public about the *actual* operational details. Accordingly, although we do not believe that Section 702 should be modified, it behooves the government to have a more robust public dialogue about the operations conducted under the statute. The Privacy and Civil Liberties Oversight Board's *Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act* in 2014 was the first significant step toward transparency and open debate. We hope that this paper has continued to contribute to that dialogue and that the public has a better understanding about this complex and vital national intelligence program.

NOTES

1 National Security Agency, "The National Security Agency: Missions, Authorities, Oversight and Partnerships," August 9, 2013.

2 Jennifer Stisa Granick and Christopher Jon Sprigman, "The Criminal N.S.A.," *New York Times,* June 27, 2013.

3 US Constitution, Tenth Amendment.

4 http://fas.org/irp/congress/2012_rpt/faa-sjc.html.

5 "[T]he title of a statute and the heading of a section are tools available for the resolution of a doubt about the meaning of a statute." Almendarez-Torres v. United States, 523 US 224, 234 (1998) (internal quotation marks omitted).

6 Foreign Intelligence Surveillance Act, 50 U.S.C. 1801(h)(1).

7 H.R. Rep. 112-645, August 2, 2012, 3.

8 See, e.g., Nadia Kayyali, "The Way the NSA Uses Section 702 is Deeply Troubling. Here's Why," Electronic Frontier Foundation, May 7, 2014.

9 United States v. Bin Laden, 126 F. Supp. 2d 264 (S.D.N.Y. 2000); see also *Warrantless Surveillance and the Foreign Intelligence Surveillance Act: The Role of Checks and Balances in Protecting Americans' Privacy Rights, Hearing before the H. Judiciary Comm., 110th Cong.,* (2007) (statement of Rep. Randy Forbes, R-VA: "The intelligence community cannot possibly know ahead of time who these terrorists will talk to. It needs to have the flexibility to monitor calls that may occur between a foreign terrorist and a person inside the United States.").

10 At 50 USC 1805; see Privacy and Civil Liberties Oversight Board, *Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act* (PCLOB Report), July 2, 2014, 6.

11 PCLOB Report, 106.

12 Due to the authors' areas of expertise—and for the sake of brevity—this paper focuses on the NSA's implementation of Section 702.

13 Barton Gellman, "U.S. Intelligence Mining Data from Nine U.S. Internet Companies in Broad Secret Program," *Washington 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, December 17, 2015.

14 Swire, "U.S. Surveillance Law," 15.

15 50 U.S.C. § 1881a(a).

16 Ibid.

17 Ibid., § 1881a(b)(1).

18 Ibid., § 1881a(b)(2).

19 Ibid., § 1881a(b)(3).

20 Ibid., § 1881a(b)(4).

21 Ibid., § 1881a(b)(5).

22 Ibid., § 1881a(g).

23 Ibid., § 1881a(g)(2).

24 PCLOB Report, 25.

25 50 U.S.C. 1881a(i).

26 NSA Director of Civil Liberties and Privacy Office, "NSA's Implementation of Foreign Intelligence Surveillance Act Section 702" (DCLPO Report), April 16, 2014, 4.

27 Ibid.

28 DCLPO Report, 4.

29 PCLOB Report, 44.

30 DCLPO Report, 4.

31 US Department of Justice and Office of the Director of National Intelligence, "Semiannual Assessment of Compliance with Procedures and Guidelines Issued Pursuant to Section 702 of the Foreign Intelligence Surveillance Act, Submitted by the Attorney General and the Director of National Intelligence" (unclassified), August 2013, A-5.

32 PCLOB Report, 46.

33 PCLOB Report, 36–37.

34 Ibid, 37.

35 Ibid.

36 Ibid.

37 Judge John Bates, FISC Opinion, 34, note 32, www.dni.gov/files/documents/1118/CLEANEDPRTT%202.pdf.

38 Bates FISC Opinion, 28.

39 PCLOB Report, 39.

40 Bates FISC Opinion, 36.

41 Mark Rumold, "What It Means to Be an NSA 'Target': New Information Shows Why We Need Immediate FISA Amendments Act Reform," Electronic Frontier Foundation, August 8, 2013.

42 *FISA Amendments Act Reauthorization: Hearing Before the House Permanent Select Committee on Intelligence* (Joint Statement of Lisa O. Monaco, assistant attorney general for national security; John C. Inglis, deputy director, NSA; and Robert S. Litt, general counsel, Office of the Director of National Intelligence), December 8, 2011, 7.

43 Bates FISC Opinion, 29–30.

44 DCLPO Report, 6.

45 Ibid.

46 NSA, "Minimization Procedures Used by the National Security Agency," July 2014, 3, https://archive.org/stream/716942-exhibit-b/716942-exhibit-b_djvu.txt.

47 Ibid., 8.

48 Ibid., 4–6.

49 See, e.g., Barton Gellman, Julie Tate, and Ashkan Soltani, "In NSA-Intercepted Data, Those Not Targeted Far Outnumber the Foreigners Who Are," *Washington Post,* July 5, 2014.

50 See, e.g., Laura K. Donohue, "Section 702 and the Collection of International Telephone and Internet Content," Georgetown University Law Center, 2014, 37 ("The NSA may thus query data obtained under §702 by using the names, titles, or addresses of U.S. persons, or any other information that may be related to the individual and his or her activities. Thus, for instance, if the intelligence community would like to query the data based on membership in the Council of Foreign Relations, on the grounds that such queries are likely to yield foreign intelligence information, it may now do so.").

51 NSA July 2014 Minimization Procedures, 6.

52 DCLPO Report, 7.

53 Director of National Intelligence, "New Privacy Protections for Information Collected Under Section 702," February 2015.

54 PCLOB Report, 57.

55 NSA July 2014 Minimization Procedures, 4–5.

56 Ibid.

57 Ibid., 1.

58 Ibid., 6.

59 Ibid., 12.

60 DOJ, "Semiannual Assessment of Compliance," 17.

61 NSA July 2014 Minimization Procedures, 9–10.

62 Ibid.

63 Ibid., 7, 11.

64 Ibid., 7.

65 DCLPO Report, 4.

66 At www.aclu.org/files/natsec/nsa/20130816/Lesson%204%20-%20So%20you%20got%20US%20Person%20Information.pdf.

67 Geoffrey Stone, "What I Told the NSA," *Huffington Post,* March 31, 2014, www.huffingtonpost.com /geoffrey-r-stone/what-i-told-the-nsa_b_5065447.html.

68 DOJ, "Semiannual Assessment of Compliance."

69 PCLOB Report, 74.

70 50 U.S.C. § 1881a(l)(2).

71 PCLOB Report, 71–74.

72 50 U.S.C. § 1881f.

73 Ibid.

74 See, e.g., *Strengthening Privacy Rights and National Security: Oversight of FISA Surveillance Programs,* Hearing of the Senate Judiciary Committee, July 31, 2013.

75 PCLOB Report ,75–76.

76 Bates FISC Opinion, 5.

77 Ibid., 7.

78 Ibid., 61.

79 Ibid., 62.

80 PCLOB Report, 65.

81 Monaco, Joint Statement.

82 White House, "Remarks by the President in a Press Conference," August 9, 2013.

83 PCLOB Report, 108.

84 Ibid.

85 Ibid.

86 James O'Toole, "Gov't Claims Spying Programs Stopped Plot to Bomb New York Stock Exchange," CNN, June 18, 2013.

87 PCLOB Report, 109; see also US House of Representatives Permanent Select Committee on Intelligence, "Four Declassified Examples," http://intelligence.house.gov/1-four-declassified-examples-more-50 -attacks-20-countries-thwarted-nsa-collection-under-fisa-section.

88 PCLOB Report, 109.

89 House Committee on Intelligence, "Four Declassified Examples."

90 See US Department of Justice, "David Coleman Headley Sentenced to 35 Years in Prison for Role in India and Denmark Terror Plots," January 24, 2013.

91 The President's Review Group on Intelligence and Communications Technologies, *Liberty and Security in a Changing World,* December 12, 2013, 145.

92 See, e.g., Electronic Frontier Foundation, "Section 702 of the Foreign Intelligence Surveillance Act (FISA): Its Illegal and Unconstitutional Use" ("The surveillance is similar to the hated British general warrants—broad and vague warrants used against American colonists—which led to the Fourth Amendment.").

93 See, e.g., United States v. Muhtorov, Case 1:12-cr-00033 (D. Colo. November 19, 2015); United States v. Mohamud, Case No. 3:10-CR-00475 (D. Or. June 24, 2014); Opinion of Judge Thomas Hogan, Foreign Intelligence Surveillance Court, August 26, 2014, 40.

94 US Constitution, Fourth Amendment (emphasis added).

95 United States v. Verdugo-Urquidez, 494 U.S. 259, 267 (1990).

96 In Re Directives, 551 F.3d 1004, 1015 (Foreign Intelligence Surveillance Court of Review 2008).

97 Griffin v. Wisconsin, 483 U.S. 868, 873 (1987) (internal quotation omitted).

98 In Re Directives, 551 F.3d 1004, 1011 (Foreign Intelligence Surveillance Court of Review 2008).

99 Bates FISC Opinion, 69 ("The government's revelation that NSA acquires MCTs as part of its Section 702 upstream collection does not disturb the Court's prior conclusion that the government is not required to obtain a warrant before conducting acquisitions under NSA's targeting and minimization procedures.").

100 United States v. Mohamud, Case No. 3:10-CR-00475 (D. Or. June 24, 2014), 31.

101 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.").

102 Wyoming v. Houghton, 526 U. S. 295, 300 (1999).

103 Opinion of Judge Hogan (internal quotations omitted).

104 NSA, "Missions, Authorities," 4.

105 Haig v. Agee, 453 U.S. 280, 307 (1981) (internal quotations omitted).

106 PCLOB Report, 92.

107 US v. Muhtorov.

108 Case No. 4:08-cv-4373 (N.D. Cal.).

109 Compl. at ¶¶ 2, 9.

110 Swire, "U.S. Surveillance Law," 17–18.

111 S. Rep. No. 112-174, 2 (June 7, 2012).

112 Winston Maxwell and Christopher Wolf, "A Sober Look at National Security Access to Data in the Cloud," white paper, 1, www.hldataprotection.com/files/2013/05/A-Sober-Look-at-National-Security-Access-to-Data-in-the-Cloud.pdf.

The preferred citation for this publication is:
Chris Inglis and Jeff Kosseff, *In Defense of FAA Section 702: An Examination of Its Justification, Operational Employment, and Legal Underpinnings,* Hoover Working Group on National Security, Technology, and Law, Series Paper No. 1604 (April 27, 2016), available at https://www.lawfareblog.com/defense-faa-section-702-examination-its-justification-operational-deployment-and-legal-underpinnings.

About the Authors

CHRIS INGLIS

Chris Inglis is the US Naval Academy's Robert and Mary Looker Distinguished Chair for Cyber Studies. He served at NSA from 1986–2014, including service as its deputy director from 2006–2014.

JEFF KOSSEFF

Jeff Kosseff is an assistant professor of cybersecurity law at the US Naval Academy. He practiced cybersecurity law at Covington & Burling and clerked for Judge Milan D. Smith Jr. on the Ninth Circuit and Judge Leonie M. Brinkema in the Eastern District of Virginia. He is an ex-journalist and was a finalist for the Pulitzer Prize for national reporting.

Jean Perkins Foundation Working Group on National Security, Technology, and Law

The Working Group on National Security, Technology, and Law brings together national and international specialists with broad interdisciplinary expertise to analyze how technology affects national security and national security law and how governments can use that technology to defend themselves, consistent with constitutional values and the rule of law.

The group focuses on a broad range of interests, from surveillance to counterterrorism to the dramatic impact that rapid technological change—digitalization, computerization, miniaturization, and automaticity—are having on national security and national security law. Topics include cybersecurity, the rise of drones and autonomous weapons systems, and the need for—and dangers of—state surveillance. The working group's output, which includes the Aegis Paper Series, is also published on the *Lawfare* blog channel, "Aegis: Security Policy in Depth," in partnership with the Hoover Institution.

Jack Goldsmith and Benjamin Wittes are the cochairs of the National Security, Technology, and Law Working Group.

For more information about this Hoover Institution Working Group, visit us online at http://www.hoover.org/research-teams/national-security-technology-law-working-group.

Hoover Institution, Stanford University
434 Galvez Mall
Stanford, CA 94305-6003
650-723-1754

Hoover Institution in Washington
The Johnson Center
1399 New York Avenue NW, Suite 500
Washington, DC 20005
202-760-3200

HOOVER INSTITUTION