Secrecy and Society **ISSN: 2377-6188**

Volume 2
Number 1 *Secrecy and Intelligence* Article 2

September 2018

Secrets and Lies — Exposed and Combatted: Warrantless Surveillance Under and Around the Law 2001-2017

Patrice McDermott
Government Information Watch, pmcdermott@govinfowatch.net

Secrets and Lies — Exposed and Combatted: Warrantless Surveillance Under and Around the Law 2001-2017

Abstract
Before June 2013, civil society and much of Congress were largely in the dark about the extent of the surveillance activities of the National Security Agency and the circumlocutions of statute undertaken by the White House and the Department of Justice. After the releases by Edward Snowden to specific journalists, the mendacity of Intelligence Community lawyers and leaders, the evasions of the law and manipulation of the FISA Court by the White House working with the Justice Department, and the scope of the violations of the Fourth Amendment protections of U.S. Persons (USPs) became increasingly apparent.2 This article reviews the changes that were initiated in the Executive Branch (and to a lesser extent in the Legislative Branch), the role civil society played in pushing and utilizing greater transparency, and what the changes mean for government accountability to the public.

Keywords
congressional oversight, Executive Order 12333, FISA, FISC, Foreign Intelligence Surveillance Act, Foreign Intelligence Surveillance Court, Michael Hayden, Intelligence Community, National Security Agency, national security intelligence, NSA, President's Surveillance Program, Edward Snowden, U.S. Department of Justice, warrantless surveillance

Secrets and Lies - Exposed and Combatted: Warrantless Surveillance Under and Around the Law, 2001–2017

Patrice McDermott[1]

Abstract
Before June 2013, civil society and much of Congress were largely in the dark about the extent of the surveillance activities of the National Security Agency and the circumlocutions of statute undertaken by the White House and the Department of Justice. After the releases by Edward Snowden to specific journalists, the mendacity of Intelligence Community lawyers and leaders, the evasions of the law and manipulation of the FISA Court by the White House working with the Justice Department, and the scope of the violations of the Fourth Amendment protections of U.S. Persons (USPs) became increasingly apparent.[2] This article reviews the changes that were initiated in the Executive Branch (and to a lesser extent in the Legislative Branch), the role civil society played in pushing and utilizing greater transparency, and what the changes mean for government accountability to the public.

Keywords congressional oversight, Executive Order 12333, FISA, FISC, Foreign Intelligence Surveillance Act, Foreign Intelligence Surveillance Court, Michael Hayden, Intelligence Community, National Security Agency, national security intelligence, NSA, President's Surveillance Program, Edward Snowden, U.S. Department of Justice, warrantless surveillance

> *Do you think a program of this magnitude gathering information involving a large number of people involved with telephone companies could be indefinitely kept secret from the American people?" [Representative Robert] Goodlatte asked.*
>
> *"Well," ODNI general counsel Robert S. Litt said with a slight smile, "we tried."*[3]

> *Greater disclosure to the public is necessary to restore the American people's trust that intelligence activities are not only lawful and important to protecting our national security, but that they are appropriate and proportional in light of the privacy interests at stake. In the long run, our ability to protect the public requires that we have the public's support.*[4]

The two epigraphs above present the critical question at the heart of this paper: Why would or should we trust the Intelligence Community? As I lay out in the following pages, the White House, the U.S. Department of Justice, and National Security Agency (NSA) have repeatedly lied to (at a minimum, misdirected) the Foreign Intelligence Surveillance Court (FISC), Congress, and not least the American public.

In one of a number of op-eds and articles posted on the one-year anniversary of the Snowden revelation, I wrote about the possible puncturing of the protective bubble around the intelligence agencies and what needs to be done to keep it from resealing. I return to these issues at the end of this article.

> *One year ago, on June 5, 2013, Edward Snowden revealed that he had provided several reporters with access to documents he had taken from the National Security Agency. The subsequent carefully researched and thoughtfully written stories blew the lid off much of the*

secrecy that the National Security Agency, the Foreign Intelligence Surveillance Court, the Department of Justice, and the intelligence community had imposed on the communications surveillance in which our government had been engaging.

A month prior to the first disclosures, in response to the advocacy community's requests that the opinions of the FISC be declassified, Robert Litt, general counsel for the Office of the Director of National Intelligence, the Justice Department and the FISA Court averred they could not and should not be declassified; that operational details were too completely interwoven with the legal discussions for it to be possible to separate them out. As a result of the disclosures, the intelligence community has been forced to declassify and release these documents and others.

The PATRIOT Act in 2001 gave permission for the FBI to seek a court order production of records or documents - tangible things - when there were reasonable grounds to believe that the information sought is relevant to an authorized investigation of international terrorism. Over the years, we learned from a disclosure made by Snowden, this provision was used to require companies like Verizon to "produce to the National Security Agency (NSA)..., and continue production on an ongoing daily basis thereafter..., unless otherwise ordered by the court, an electronic copy of: all call detail records or "telephony metadata" created by Verizon for communications (i) between the United States and abroad; or (ii) wholly within the United States, including local telephone calls.

We learned through an administration White Paper (intended to calm the waters) that multiple FISC judges found that Section 215 authorizes such bulk collection of metadata—not to gain access to specific items about specific persons on a case-by-case basis as the law clearly states, but, rather, because technology makes it useful to a "broad range of investigations of international terrorism" - which may or may not themselves have been authorized by the FISC. Worse yet, we further learned from a declassified and released 85-page ruling by John Bates, then serving as chief judge on the FISC, that the court found that its approval of a government interpretation...was "premised

> *on a flawed depiction" of how the program operated and "buttressed by repeated inaccurate statements in the government's submissions" to the court.*
>
> *The revelations have continued to this day. As a result, legislation that makes major changes to bulk collection of call records passed the House in 2014*[5] *- although it remains possible that it, too, will be secretly interpreted to allow surveillance of millions of Americans. The director of the Office of the Director of National Intelligence has publicly accepted the need for greater transparency and taken some steps in that direction.*
>
> *The bubble that has seemed to protect the intelligence community from President Obama's openness initiatives may have sprung a leak. It is essential that, as the debate over the USA FREEDOM Act moves to the Senate, Congress ensures that this leak is not resealed, and that future disclosures should not require anyone to take the risks Snowden did. Instead, they should come from declassification of FISA court decisions, public reports of how many people's communications are being stored in the NSA's databases, and oversight hearings that are open to the press and public.*[6]

Context and Perspective

In order to understand the context for the "Snowden disclosures" and what they have meant for Executive Branch accountability, it is necessary to understand the course of efforts to rein in - or at least secure some (often minimal) oversight of - the U.S. Intelligence Community. These initiatives include the Foreign Intelligence Surveillance Act (FISA) and the amendments thereto, including, for the purposes of this article, the USA PATRIOT Act, the USA Freedom Act, and the FISA Amendments Act (FAA) and its

reauthorizations. The whole story (that we know to date) is a complicated tale, which I try to encapsulate in this article.

This article is not written from an academic perspective; it is the struggle of an engaged (non-lawyer) advocate to understand how the protections of the Fourth Amendment were violated repeatedly - and outside of scrutiny for accountability - by the U.S. Intelligence Community, especially the White House, the Department of Justice, and the NSA, and the roles of the Congress and the Foreign Intelligence Surveillance Court (FISC) in those violations. The experience has been akin to putting together a moving puzzle without an image to use as a reference (or with only a completely different image - such as what the statutes say) and with some of the pieces missing, hidden, changing shapes, or somehow deliberately obscured.

An integral part of the story is the engagement of civil society - privacy, civil liberties, and open government organizations - in pushing back against the Executive Branch (including through Freedom of Information Act [FOIA] litigation) and in working with (and often also pushing back on) Congress. The output of civil society has been deeply informed and informative - and voluminous. For that reason, I have put as many as I could locate of the letters, statements to/testimony before congressional committees (ranging from 2002 to 2018), and commentaries (specifically on

the 2017 reauthorization FISA Amendment) on a separate website. The links are here.[7]

The dedicated reporters, all the individuals behind the scenes, and the editors of numerous newspapers and news sites have been - and continue to be - irreplaceable guides to the documents, the context, and the analysis of the programs as unveiled to the public. At the end, I will try to point to some initiatives to keep the leak in the Intelligence Community's bubble of secrecy from being resealed. It was a difficult task in an administration committed (at least rhetorically) to transparency; it may well prove to be Sisyphean in the current administration.

It is worth noting that, as of this writing, the ODNI is continuing to declassify and release documents. Although these are quite often in response to court orders (e.g., in FOIA litigation), some seem more voluntary. Members of Congress have recently passed legislation to address some of the most egregious abridgements of constitutional protections—but ongoing oversight will be necessary.

The secret Foreign Intelligence Surveillance Court also needs reform and greater transparency. In the case of Congress and its responsibility for oversight of the Intelligence Community (IC), it needs greater substantive and consequential accountability to the American public. It also needs greater internal transparency. The basic organization of the article is:

1. A discussion of the text and the intent of the legislation indicated at the beginning of each section (including a section on the extra-

legislative "President's Surveillance Program" and one on Executive Order 12333); the Foreign Intelligence Surveillance Act; Executive Order 12333; the USA PATRIOT Act; USA PATRIOT Act Improvement and Reauthorization Act of 2005; the President's Surveillance Program[8]; Section 702 of the 2008 Foreign Intelligence Surveillance Amendments Act; the USA FREEDOM Act; and the 2017 Foreign Surveillance Amendments Act Reauthorization;

2. What has been revealed as a result of the disclosures made by Edward Snowden;

3. How civil society and, where known, the courts and Congress used the revelations to enact changes in law and/or practice.

These topics are followed by discussions of the problems with congressional and FISA Court oversight.

Foreign Intelligence Surveillance Act of 1978

The Foreign Intelligence Surveillance Act of 1978 (FISA) was one of the results of a scandal that exposed a wide range of intelligence abuses by federal agencies, including the CIA, FBI, Internal Revenue Service, and National Security Agency. The abuses were (and continue to be) constitutional; the Fourth Amendment guarantees

> 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.

Background

In 1973, the Senate Watergate Committee investigation revealed that the Executive Branch had directed national intelligence agencies to carry out constitutionally questionable domestic security operations. Following a 1974

front-page *New York Times* article by Seymour Hersh,[9] claiming that the CIA had been spying on anti-war activists for more than a decade and thus violating the agency's charter, former CIA officials and some lawmakers called for a congressional inquiry.

According to Senate history, on January 21, 1975, Senator John Pastore introduced a resolution (passed by the Senate 82-4) to establish a select committee to investigate federal intelligence operations and determine "the extent, if any, to which illegal, improper, or unethical activities were engaged in by any agency of the Federal Government."[10] Majority Leader Mike Mansfield and Republican leader Hugh Scott carefully selected committee members; Mansfield selected as chairman Democrat Frank Church of Idaho, a sixteen-year member of the Committee on Foreign Relations, who had co-chaired a special committee to critically examine the executive branch's consolidation of power in the Cold War era. According to the Senate history of the commission, Church recognized the strategic value of the nation's top intelligence agencies and was also mindful of the need for American institutions to function within the confines of US constitutional law.[11]

The Church Committee conducted a far-reaching Senate investigation into U.S. intelligence agencies, and in the course of their work, investigators identified programs - never before known to the public - that monitored wire communications to and from the United States and shared some of that data

with other intelligence agencies, including NSA's Projects SHAMROCK and MINARET.[12]

Over a nine-month period, the committee interviewed hundreds of witnesses and conducted numerous hearings, ultimately producing analysis demonstrating that the FBI had engaged in illegal covert operations in the United States, and that the CIA had engaged in illegal covert operations at home and abroad. As Scott Boykin notes, the Committee's reports demonstrated that the FBI and CIA had harassed civil rights and political dissident groups, opened and read individuals' mail, and conducted warrantless break-ins to plant surveillance devices and steal information regarding the groups' members.[13,14]

In its final report, the Committee included 96 recommendations, both legislative and regulatory, designed "to place intelligence activities within the constitutional scheme for controlling government power."[15,16] The committee observed that "there is no inherent constitutional authority for the President or any intelligence agency to violate the law," and recommended strengthening oversight of intelligence activities.

In 1976, the Senate approved Senate Resolution 400, establishing the *Senate Select Committee on Intelligence, to provide "vigilant legislative oversight over the intelligence activities of the United States to assure that such activities are in conformity with the Constitution and laws of the United States*" [emphasis added].[17,18] The Committee's reports helped prompt

significant legislative reforms, including the Foreign Intelligence Surveillance Act of 1978, signed into law by President Jimmy Carter.[19]

The FISA Court Established

The law required the Executive Branch to request warrants for wiretapping and surveillance purposes from a newly formed FISA Court. Under the statute as adopted, the President could authorize electronic surveillance of foreign powers to gather intelligence upon the Attorney General's certification that there was no "substantial likelihood" that the government would obtain the communications of a "United States person," or USP, a citizen or other lawful resident of the United States,[20] and that the minimization procedures for the surveillance protected the private information of USPs.[21]

The newly created FISA Court could issue orders for electronic surveillance of foreign powers or their agents upon application by federal officers authorized by the Attorney General on behalf of the President. A USP could not be regarded as a foreign power for purposes of obtaining an order from the FISC for activities protected by the First Amendment. A USP could be an agent of a foreign power when: the person engages in clandestine intelligence activities on a foreign power's behalf; such activities may involve a violation of the criminal laws of the United States; a person engages or prepares to engage in sabotage or international terrorism on behalf of a

foreign power; a person enters the United States under a false identity on behalf of a foreign power; or a person aids or abets or conspires to do any of the foregoing. Under FISA, the location of the surveillance *must be a place that is to be used by a foreign power or its agent.* The FISC order for surveillance had to *specify the target and location, the method of conducting it, its duration, and the number of devices employed.* The required minimization procedures *had to meet the same requirement as for electronic surveillance without a court order.*

Each of these requirements has been undermined in the ensuing years.

The Erosion of Fourth Amendment Protections

In the history of the erosion of the Fourth Amendment protections post-FISA, it is important to note that many of the erosions undertaken by the Executive Branch did not have the sanction of legislation.

Executive Order 12333[22]

The Order, signed by President Ronald Reagan on December 4, 1981, established broad new surveillance authorities for the intelligence community and governs the NSA's signals intelligence collection abroad; it is outside the scope of public law.[23] The Order was most recently amended on January 3, 2017. It is discussed in detail below.

The timing of the Order is not coincidental:

> At the time the order was written, the nation's intelligence community was dealing with a shattered reputation after decades of widespread abuses. The Church Committee—a special congressional panel tasked in the 1970s with investigating intelligence abuses—had revealed CIA efforts to cover up the Watergate scandal, the CIA's opening of Americans' mail, and the agency's efforts to assassinate Cuba's Fidel Castro.
>
> Executive Order 12333 was intended to bolster a reeling intelligence community and further define its authority to conduct foreign intelligence gathering.
>
> The global telecommunications network didn't exist, and collecting foreign communications posed little risk for Americans' data to be swept up in the dragnet.[24]

The President's Surveillance Program

The Bush Administration stacked the deck *before* the passage of the PATRIOT Act. The "President's Surveillance Program" (PSP) operated in secrecy for approximately seven years.[25]

I will return to the PSP after the discussion of the USA PATRIOT Act (and its Reauthorization), because while Congress and the Bush Administration intended the USA PATRIOT Act to strengthen the nation's ability to combat terrorism after the 9/11 attacks, *the Bush administration also was convinced that it needed to avoid FISA's requirements that it obtain judicial approval for surveillance activities*. The PSP was its solution, and *Executive Order 12333* ("E.O. 12333," discussed below) was the vehicle.[26]

The Program consisted of warrantless surveillance on persons the Bush administration suspected might be involved in terrorist activities. Beginning in 2001, the government intercepted international phone calls, and the

NSA's STELLARWIND program mined information from email databases and gathered telephone metadata from the databases of cellphone service providers.[27,28] The NSA also gathered and analyzed the content of telephone conversations and email communications from these databases and, from the beginning of the PSP through January 2007, eight percent of the communications analyzed were those of USPs. The PSP was the first post-2001[29] example of the focus of this article: Warrantless Surveillance Under and Around the Law - in this case, completely around. President Bush did not ask Congress to include provisions for the NSA domestic surveillance program as part of the USA PATRIOT Act and did not seek any other laws to authorize the operation. Bush administration lawyers argued that such new laws were unnecessary, because they believed that the Congressional resolution on the campaign against terrorism provided ample authorization. The program was initially based on the executive's "inherent power" to gather foreign intelligence. After internal dissent, an additional rationale was added: Congress's resolution authorizing the wars in Iraq and Afghanistan included the implicit authority to capture communications related to those areas.[30,31]

Even though the Program started before the passage of the PATRIOT Act, it is important to first understand what that law, enacted by Congress, permitted the Department of Justice and the NSA to do in terms of collecting, mining, and analyzing the communication records of USPs, and

what the public and much of Congress believed were the limitations on the government's surveillance.[32] First, though, I begin with Executive Order 12333, as it is behind the bulk and warrantless surveillance occurring since its inception, but little discussed. After that discussion, I go to the first legislative amendments to the FISA: the USA PATRIOT Act.

Issuance and Effects of Executive Order 12333

The NSA's collection of information on Americans' cellphone and Internet usage reaches far beyond the two programs that have received public attention (PRISM[33] and "Upstream"), to a presidential order "that is older than the Internet itself."[34,35]

Indeed, documents leaked by former NSA contractor Edward Snowden suggest that less than half of the metadata the NSA has collected has been acquired under provisions of the USA PATRIOT Act and FISA, the two laws that have received the most attention for permitting NSA programs: "Gen. Keith Alexander, the (then) NSA director, has ratified that impression, saying that the majority of NSA data is collected 'solely pursuant to the authorities provided by Executive Order 12333.'"[36]

Executive Order 12333,[37] approved by President Ronald Reagan in 1981, to this day governs most of what the NSA does, outlines the duties and foreign intelligence collection for the nation's 17 intelligence agencies,

and remains the primary authority under which the country's intelligence agencies conduct the majority of their operations.[38]

Under its provisions, agencies have the ability to *function outside the confines of a warrant or court order, if approved by the attorney general*. Its Section 2.5 effectively gives the attorney general the right to authorize intelligence agencies to operate outside the confines of judicial or congressional oversight, so long as it is in pursuit of foreign intelligence—including collecting information of Americans: "The Attorney General hereby is delegated the power to approve the use for intelligence purposes, within the United States or against a United States person abroad, of any technique for which a warrant would be required."[39]

Monitoring the actual content of Americans' communications still requires a warrant, but metadata - the hidden information about a communication that tells where a person is, with whom he's communicating, even the number of credit cards used in a transaction - can be swept up without congressional or court approval. The Order is not governed by Congress, and what changes have been made to it have come through guidelines set by the Attorney General or other documents.[40] The result is a "web of intelligence law so complicated that it stymies even those tasked with interpreting it. As one former executive official said, 'It's complicated stuff.'"[41]

Outdated Agency Guidelines Do Not Protect Metadata

Intelligence officials have said that each agency's respective 12333 collection is governed by supplemental guidelines written by the attorney general, and that those guidelines protect Americans' data. They admitted in 2013, however, that most of those guidelines had not been revisited in decades, and that they don't offer the same protections as the metadata collection programs authorized under the PATRIOT Act and FISA. At that time, they wrote:

> NSA uses EO 12333 authority to collect foreign intelligence from communications systems around the world. Due to the fragility of these sources, providing any significant detail outside of classified channels is damaging to national security. Nonetheless, every type of collection undergoes a strict oversight and compliance process internal to NSA that is conducted by entities within NSA other than those responsible for the actual collection.
>
> NSA has an internal oversight and compliance framework to provide assurance that NSA's activities - its people, its technology, and its operations - act consistently with the law and with NSA and U.S. intelligence community policies and procedures. This framework is overseen by multiple organizations external to NSA, including the Director of National Intelligence, the Attorney General, the Congress, and for activities regulated by FISA, the Foreign Intelligence Surveillance Court.[42]

As noted, neither the regular federal courts nor the Foreign Intelligence Surveillance Court, which is tasked with approving some forms of surveillance, provide meaningful or accountable oversight of EO 12333 activities. The FISC is required to authorize and oversee collection activities conducted pursuant to FISA, to assess sufficiency of IC foreign intelligence

procedures, and to receive compliance reports from the IC concerning only *violations of FISA,* not other violations of the 4th Amendment by the IC.[43]

Lack of Protections and Bulk Data Collection

Senator Dianne Feinstein, then-chair of the Senate Select Committee on Intelligence, noted that the Order has few, if any, privacy protections: "I don't think privacy protections are built into it. It's an executive policy. The executive controls intelligence in the country."[44]

To this point, it is important to note (as is done below in the discussions of legislation) that bulk data collection that occurs inside the United States must be authorized by statute, has some protections of the privacy of USPs, and is subject to oversight from Congress and the Foreign Intelligence Surveillance Court. Executive Order 12333, however, contains no such protections for USPs if the collection occurs outside U.S. borders; it authorizes collection of the content of communications, not just metadata, even for USPs.[45,46] Although such persons cannot be individually targeted under 12333 without a court order, if the contents of a USP's communications are "incidentally" collected (an NSA term of art) in the course of a lawful overseas foreign intelligence investigation, then Section 2.3(c) of the executive order explicitly authorizes their retention. It does not require that the affected USPs be suspected of wrongdoing and places no

limits on the volume of communications by USPs that may be collected and retained.[47]

We do know a little about the spying conducted using EO 12333. In November 2013, a *Washington Post* report revealed EO 12333 was the NSA's claimed authority for the collection of Americans' address books and buddy lists - as the Electronic Frontier Foundation (EFF) put it, the NSA has been siphoning off data from the links between Yahoo! and Google data centers, which include the fiber optic connections between company servers at various points around the world. As noted above, the NSA has not been authorized by Congress or the FISC to collect contact lists in bulk, and senior intelligence officials said it would be illegal to do so *from facilities in the United States*.[48,49,50,51]

> One official, speaking on the condition of anonymity to discuss the classified program, said the agency avoids the restrictions in the Foreign Intelligence Surveillance Act by intercepting contact lists from access points "all over the world. None of those are on U.S. territory."
>
> Because of the method employed—when information passes through "the overseas collection apparatus," the official added, "the assumption is you're not a U.S. person"—the agency is not legally required or technically able to restrict its intake to contact lists belonging to specified foreign intelligence targets, he said.

A senior U.S. intelligence official told the Post that the privacy of Americans is protected, despite mass collection, because "we have checks and balances built into our tools."[52]

The most recent change to the Order came from President Barack Obama in the final days of his administration. The new rules let the NSA

share the raw streams of communications it intercepts directly with agencies including the FBI, the DEA, and the Department of Homeland Security.

According to Robert S. Litt, the then-general counsel to the Director of ODNI, "This is not expanding the substantive ability of law enforcement to get access to signals intelligence. It is simply widening the aperture for a larger number of analysts, who will be bound by the existing rules."[53]

And they have checks and balances built into their tools.

The USA PATRIOT Act

Less than a week after the terrorist attacks of September 11, 2001, legislative proposals to strengthen the nation's ability to combat terrorism after the attacks and to give broad new powers to the Executive Branch - with relatively little oversight from the courts - were introduced. President Bush signed the final bill, the USA PATRIOT[54] Act (Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, P.L. 107-56),[55] into law on October 26, 2001. Although the Act made significant amendments to more than 15 important statutes - in particular, the Foreign Intelligence Surveillance Act of 1978 (FISA)[56] and the Electronic Communications Privacy Act of 1986 (ECPA)[57] - it was introduced with great haste and passed with little debate, and without a House, Senate, or conference report.[58] The Act thus lacks background legislative history that often retrospectively provides the necessary material

to guide statutory interpretation.

Section 215 of the USA PATRIOT Act

Title II of the PATRIOT Act made a number of significant changes to the laws relating to foreign intelligence surveillance, appreciably expanding government investigative authority. Specifically, Section 215 substantially revised the authority under the FISA.[59] It amended Title V of the FISA by striking sections 501 through 503 of that act and inserting - as Section 215 - the following: SEC. 501, Access to Certain Business Records for Foreign Intelligence and International Terrorism Investigations, discussed below; and SEC. 502 on Congressional Oversight.[60]

- *What Kind of Records?* Under the (unamended) FISA, the FISA Court (FISC) could issue orders for *electronic surveillance* of foreign powers or their agents. Section 215 broadened the government's authority by eliminating any limitation on the types records that may be seized:

  (a)(1) The Director of the Federal Bureau of Investigation or a designee of the Director (whose rank shall be no lower than Assistant Special Agent in Charge[61]) may make an application for an order requiring the production of *any tangible things* (including books, records, papers, documents, and other items) for an investigation to protect against international terrorism or clandestine intelligence activities.

- *With What Authorization?* Under the FISA,[62] a judge having jurisdiction[63] could issue orders for electronic surveillance of foreign powers or their agents upon application by federal officers authorized

by the Attorney General on behalf of the President, upon the Attorney General's certification that there was no "substantial likelihood" that the government would obtain the communications of a USP (a citizen or other lawful resident of the United States), and that the private information of USPs was protected by the minimization procedures for the surveillance.

Section 215 shifts the authorization from the Attorney General to the Director of the Federal Bureau of Investigation or a designee of the Director (of a rank no lower than Assistant Special Agent in Charge).

- *For Whose Records?* Under the FISA, a USP could not be regarded as a foreign power for purposes of obtaining an order from the FISC for activities protected by the First Amendment.

  Section 215 states that an investigation conducted under this section should be conducted under guidelines approved by the Attorney General under Executive Order 12333 (or a successor order); and not "be conducted of a United States person solely upon the basis of activities protected by the first amendment to the Constitution of the United States."

  The incorporation of Section 501 of the FISA into Section 215 of the PATRIOT Act permitted the FBI to apply to the Foreign Intelligence Surveillance Court (FISC) for an order to seize business records of

hotels, motels, car and truck rental agencies, and storage rental facilities.

- *For What Purposes?* Under the FISA, an application for an order allowing electronic surveillance required a statement of a federal officer under oath attesting to the identity or description of a proposed target for surveillance, a statement of the "facts and circumstances" showing that the target is "being used or is about to be used" by "a foreign power or an agent of a foreign power," a description of the communications sought and the types of communications being sought, and "that a *significant purpose* of the surveillance is to obtain foreign intelligence information" that cannot be obtained by ordinary intelligence-gathering techniques [emphasis added].

"Foreign intelligence information" in the FISA (unamended) is limited to that needed to protect the United States against hostile acts, terrorism, or intelligence operations directed against the United States by a foreign power or its agent. A judge must find that there is probable cause showing that the target of the surveillance is a foreign power or its agent, and that the facilities targeted are being used or are about to be used by a foreign power or its agent.[64]

As noted earlier, under the FISA, the location of the surveillance must be a place that is to be used by a foreign power or its agent. The FISC order for surveillance had to specify the target and location, the method of

conducting it, its duration, and the number of devices employed. The minimization procedures had to meet the same requirement as for electronic surveillance without a court order.

Section 215 only required the government to assert that the records or other things are ”sought for an authorized investigation conducted in accordance with subsection (a)(2) to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities.”[65] The terms “foreign intelligence information” and “international terrorism” are undefined. There is no requirement for an evidentiary or factual showing and the judge has little discretion in reviewing an application, nor is there the limitation on place.

Section 505 of the USA PATRIOT Act

Section 505 allowed the use of National Security Letters (NSLs) when seeking information "relevant" in authorized national security investigations to protect against international terrorism or clandestine intelligence activities. A National Security Letter is a type of administrative subpoena: a written demand from the FBI that compels Internet service providers (ISPs), credit companies, financial institutions, and others to hand over confidential records of their customers, including, but not limited to, subscriber information, phone numbers and email addresses, and websites visited. The

recipient of the order may not disclose the fact that the FBI has sought or obtained records.[66]

- *Who authorizes such Letters?* As long as the head of an FBI field office certifies that the records would be relevant to a counterterrorism investigation, the Bureau can send a National Security Letter request without the approval of a judge or grand jury - it is not a warrant.

The USA PATRIOT Act was modified by the USA PATRIOT Act Improvement and Reauthorization Act of 2005 (immediately below) and the USA FREEDOM Act (discussed later).

USA PATRIOT Act Improvement and Reauthorization Act of 2005

The American Library Association, the American Civil Liberties Union, Bill of Rights Defense Committee, and many others were engaged over a number of years in pushing in public and in Congress for changes to the USA PATRIOT Act to protect privacy and civil liberties.[67] The reauthorizing legislation addressed a number of concerns of the privacy and civil liberties communities.

Section 215 orders:

- A Section 215 order cannot be issued unless the information sought is relevant to (rather than just "sought for") an authorized national security investigation (other than a threat assessment).
- The FISA court is allowed to issue a section 215 order for certain more sensitive categories of documents—such as library, bookstore, medical, tax return, and gun sale records. The application must be signed by either the Director or Deputy Director of the FBI (rather than

a designee of the Director (of a rank no lower than Assistant Special Agent in Charge).

- It requires the Attorney General to develop and apply "minimization procedures" limiting the retention and dissemination of information concerning USPs obtained through section 215 orders - thus restoring a requirement under the original FISA.

- It allows explicit judicial review of NSLs and any accompanying nondisclosure orders, and provides that nondisclosure orders no longer automatically attach to NSL requests.

- It clarifies that a recipient may disclose receipt of an NSL to those necessary to comply with it, or to an attorney in order to obtain legal advice or assistance with respect to it.

- It explicitly allows recipients to seek judicial review, to disclose receipt of a 215 order to attorneys in order to obtain legal advice or assistance, and to other people necessary to comply with the request.

Section 206 roving surveillance orders: This Section allows the FISC to issue an electronic surveillance order that attaches to a particular *target,* rather than to a particular phone or computer. It clarifies the level of detail necessary to obtain a section 206 order, particularly where the target is identified by a description rather than by name.[68]

Sunsetted Provisions: The reauthorizing legislation made permanent 14 of the 16 sunsetted USA PATRIOT Act provisions. It placed four-year sunsets on the other two - the authority to conduct "roving" surveillance under the FISA; and the authority to request production of business records under FISA (USA PATRIOT Act sections 206 and 215, respectively).[69]

What We Learned as a Result of the Snowden Documents[70]

The Scope of Collection under Section 215

- *FISA Court Order to Verizon to provide a broad data collection:* On June 5, 2013, we learned that Verizon (and others) were required to indiscriminately provide all[71] domestic call detail records to the NSA under an April 25, 2013 court-order.[72] This requirement was made under the auspices of Section 215, which, as written, did not authorize such an unspecific collection.

  There was a veiled indication of this use of Section 215 in 2011 when the acting head of the Justice Department's National Security Division Todd Hinnen testified that "some orders have also been used to support important and highly sensitive intelligence collection operations, on which this committee and others have been separately briefed.[73] On average, we seek and obtain section 215 orders less than 40 times per year." I return to this testimony below.

  How did we get from the Section 215 statutory language "tangible things" (as normally understood) relevant to an authorized investigation of international terrorism, to the language from the Court Order below?

  > [T]he Custodian of Records shall produce to the National Security Agency (NSA) upon service of this Order, and continue production on an ongoing daily basis thereafter for the duration of this Order, unless otherwise ordered by the Court, an electronic copy of the following tangible things: all call detail records or "telephony metadata" created by Verizon for communications (i) between the United States and

abroad; or (ii) wholly within the United States, including local telephone calls.

Before Snowden provided journalists with the FISC order to Verizon, it was assumed (with some suspicion) by the civil liberties community (and many in the media) that Section 215 was being used in discrete requests to obtain individual collections of records about known counterintelligence or terrorist suspects - "for records showing, say, that a *certain person* made *certain purchases* from a *certain vendor* or used a *particular telephone* to make *specific calls*"[74] [emphasis added].

- *FBI Director Mueller's Response re "increase in the volume of business records requests":* In a 2011 response (apparently to a congressional Questions for the Record), then-FBI Director Mueller indicated that, beginning in late 2009, certain electronic communications service providers no longer honored National Security Letters (under Section 505) to obtain records because of what their lawyers cited as "an ambiguity" in the law.[75] As a result, Mueller said, the FBI had switched over to demanding the same "business records" data under Section 215.

  According to Mueller, "This change accounts for a significant increase in the volume of business records requests." As noted above, however, Todd Hinnen's 2011 testimony suggested that these orders were comparatively rare: "we seek and obtain section 215 orders less than 40 times per year."[76]

> Before Snowden, the public was prevented from knowing that behind the small number (212 requests in 2012) of Section 215 requests, applications to the FISC "for access to certain business records (including the production of tangible things) for foreign intelligence purposes" were the massive numbers involved in the bulk collections of metadata on calls "wholly within the United States, including local telephone calls."

Administration White Paper

Through the August 2013 Administration White Paper[77], we learned that multiple FISC judges - beginning in 2006 - found that Section 215 authorizes the collection of *telephony metadata in bulk*.[78] According to the Administration, the FISC judges considered that the telephony metadata collection program meets the "relevance" standard of Section 215 because there are "reasonable grounds to believe" that this category of data, when queried and analyzed consistent with the Court-approved standards,[79] will produce information pertinent to FBI investigations of international terrorism, because

> certain analytic tools used to accomplish this objective require the collection and storage of a large volume of telephony metadata [and] … *communications metadata is different from many other kinds of records because it is inter-connected and the connections between individual data points, which can be reliably identified only through analysis of a large volume of data*, are particularly important to a broad range of investigations of international terrorism [emphasis added].[80]

So, the FBI and the NSA were authorized to get this information, not in order to gain access to specific items about specific persons on a case-by-case basis, but, rather, because technology makes it useful to a "broad range of investigations of international terrorism" - which may or may not themselves have been authorized by the FISC.

- *New NSA Term "hops"*: In 2013, a new term, "hops," was added to our vocabulary. In his testimony[81] before the House Judiciary Committee[82] NSA Deputy Director John Chris Inglis stated that *the FISA court "has approved us to go out two or three hops"* - or, as we now know, to "contact chain."[83] *The Washington Post* explained:

  > When analysts think they have cause to suspect an individual, they will look at everyone that person has contacted, called the first hop away from the target. Then, in a series of exponential ripples, they look at everyone all those secondary people communicated with. And from that pool, they look at everyone those tertiary people contacted. This is called a second and a third hop.[84]

  As members of the committee were quick to point out at the time, this is not what the law, as passed by Congress, allows.[85] Indeed, at this hearing, Representative Jerrold Nadler told Deputy Attorney General James Cole, "The statute says 'collection.' You're trying to confuse us by talking use."[86]

  And indeed, it seems that the DOJ officials were trying to do just that. Inglis and Cole actually were referring to a 2007 Justice Department memo[87] (discussed below under President's Surveillance Program), in

> which the Department of Defense (NSA) sought Attorney General approval pursuant to Executive Order 12333 of a proposed amendment to "procedures governing the National Security Agency's Signals Intelligence Activities."[88]

The NSA was quite willing to misdirect the FISC as well as Congress. As we will see below (in the President's Surveillance Program section), in a discussion of Judge Bates' Opinion - also declassified as a result of the Snowden disclosures - the FISC approval of contact chaining (hops) was sought under the various permutations of the President's/Terrorist Surveillance Program.[89]

FISA Court Documents Detailing the Court's Interpretation of Section 215

In September 2013, in response to a court order in a 2011 EFF lawsuit (see below under President's Surveillance Program, Civil Society Engagement), the government released hundreds of pages of previously secret FISA documents detailing the court's interpretation of Section 215, including an opinion excoriating the NSA for misusing its mass surveillance database for years (see below).[90]

Civil Society Engagement

The American Library Association, the American Civil Liberties Union, Bill of Rights Defense Committee, and many others were engaged over a

number of years in pushing - in public and in Congress - for changes to the USA PATRIOT Act to protect privacy and civil liberties.[91] These efforts came to some fruition in the 2005 Amendments (see above).

On October 26, 2011, EFF sued the Department of Justice (DOJ) for answers about "secret interpretations" of a controversial section of the law.[92] On June 11, 2013, the American Civil Liberties Union and the New York Civil Liberties Union filed a challenge (*ACLU v. Clapper*) with the FISC, requesting that it publish its opinions on the meaning, scope, and constitutionality of Section 215.[93,94] The organization filed its motion after *Guardian* disclosed (based on Snowden-provided documents) a secret FISC order (regarding Verizon) - issued under Section 215 of the PATRIOT Act - authorizing the bulk collection of Americans' call records.[95]

In September 2013, in response to a court order in the lawsuit, the government released hundreds of pages of previously secret FISA documents detailing the court's interpretation of Section 215, noted above.[96] In October 2013, the government released a second batch of documents related to Section 215, which showed, among other things, that the NSA had collected cell site locations without notifying its oversight committees in Congress or the FISA court.[97]

In November 2013, the ACLU and the Yale Law School's Media Freedom and Information Access (MFIA) clinic filed a second motion, seeking to uncover the legal underpinnings of the government's bulk collection of

Americans' data more broadly.[98,99]

What Has Occurred Since?

Bulk Collection under Section 215 Ruled Illegal: On May 7, 2015, in a 97-page ruling, *ACLU v. Clapper*, a three-judge panel (Gerald E. Lynch, Robert D. Stack, and Vernon S. Broderick) of the United States Court of Appeals for the Second Circuit held, on May 7, 2015, that Section 215 of the USA PATRIOT Act cannot be legitimately interpreted to allow the bulk collection of domestic calling records.[100] This ruling was the first time a higher-level court in the regular judicial system (i.e., not the FISC) reviewed the NSA phone records program.[101]

In the unanimous ruling written by Judge Gerard E. Lynch, the court held that Section 215 "cannot bear the weight the government asks us to assign to it, and that it does not authorize the telephone metadata program."[102] In declaring the program illegal, the court said, "We do so comfortably in the full understanding that if Congress chooses to authorize such a far-reaching and unprecedented program, it has every opportunity to do so, and to do so unambiguously."[103]

The ruling raised the question of whether Section 215, extended or not, has ever legitimately authorized the program.[104] The court said that the statute on its face permits only the collection of records deemed "relevant" to a national security case. Judge Lynch wrote:

> Such expansive development of government repositories of formerly private records would be an unprecedented contraction of the privacy expectations of all Americans. Perhaps such a contraction is required by national security needs in the face of the dangers of contemporary domestic and international terrorism. But we would expect such a momentous decision to be preceded by substantial debate, and expressed in unmistakable language.[105]

As discussed below, under the President's Surveillance Program, the data collection had repeatedly been approved in secret by judges serving on the FISC. Those judges heard arguments only from the government, and they accepted the interpretation of Section 215 now rejected by the appeals court.[106]

- *Renewal of Non-Permanent Provisions of the PATRIOT Act:* Three provisions of the PATRIOT Act that must be renewed periodically expired on June 1, 2015. With the passage of the USA Freedom Act (USAF) (discussed below) on June 2, 2015, these provisions were extended for four years: roving wiretaps (authorized for sometimes unnamed targets who communicate with multiple devices rather than *a* communications line or device); court-ordered searches of business records; and surveillance of non-American "lone wolf" suspects without confirmed ties to terrorist groups.[107]

  The USAF also blocks the government from transferring mass phone record collection, such as national security letter statutes or Section 214 of the PATRIOT Act, to other authorities.[108]

President's Surveillance Program (PSP)

The PSP was the first post-2001 example of the focus of this article: Warrantless Surveillance Under and Around the Law - in this case, completely around.[109] As noted earlier, while Congress and the Bush Administration intended the USA PATRIOT Act to strengthen the nation's ability to combat terrorism after the 9/11 attacks, *the Bush administration also was convinced that it needed to avoid FISA's requirements that it obtain judicial approval for surveillance activities*. The PSP was its solution, and E.O. 12333 was the vehicle.[110] President Bush did not ask Congress to include provisions for the NSA domestic surveillance program as part of the USA PATRIOT Act and did not seek any other laws to authorize the operation.

On 4 October 2001, President George W. Bush issued a memorandum entitled *Authorization For Specified Electronic Surveillance Activities During A Limited Period To Detect And Prevent Acts Of Terrorism Within The United States*. The Presidential authorization delegated authority to the Secretary of Defense, who further delegated it to the Director of National Security Agency/Chief, Central Security Service (DIRNSA/CHCSS) to conduct specified electronic surveillance on targets related to Afghanistan and international terrorism for 30 days. Because the surveillance included wire and cable communications carried out *into or out of* the United States, *it would otherwise have required FISC authority* [emphasis added].[111]

Operating Outside the Law

Although the Authorization document may seem somewhat limited, it metastasized into the President's Surveillance Program (PSP), known publicly - after two *New York Times* stories exposed it in December 2005 - as the Terrorist Surveillance Program.[112,113] It operated literally "around" and outside congressionally passed law discussed in this article (although the FISA Court and, at some point, some parts of Congress became aware of it).[114] The Authorization highlights the intent of the Bush Administration to operate surveillance activities *inside* the United States, which had been barred by law and agency policy for decades, and to do so outside the context of warrants and, thus, of the Foreign Intelligence Surveillance Court.

Within the Bush administration, Department of Justice lawyers argued that new laws were unnecessary; they believed that the congressional resolution on the campaign against terrorism provided ample authorization. The program was initially based on the executive's "inherent power" to gather foreign intelligence. After internal dissent, an additional rationale was added: Congress's resolution authorizing the wars in Iraq and Afghanistan included the implicit authority to capture communications related to those areas.[115]

Warrantless Surveillance and STELLARWIND

STELLARWIND consisted of warrantless surveillance on persons the Bush administration suspected might be involved in terrorist activities. Beginning in 2001, the government intercepted international phone calls, and the NSA's STELLARWIND program mined information from email databases and gathered telephone metadata from the databases of cellphone service providers.[116],[117] The NSA also gathered and analyzed the content of telephone conversations and email communications from these databases and, from the beginning of the PSP through January 2007, eight percent of the communications analyzed were those of USPs.

According to a 2009 Report prepared by the Inspectors General of the involved agencies (discussed in detail below), the NSA cited authorization for the President's Surveillance Program under E.O. 12333:

> For more than a decade before the terrorist attacks of 11 September 2001 ... NSA was authorized by Executive Order (E.O.) 12333, *United States Intelligence Activities,* 4 December 1981, as amended, to collect, process, and disseminate SIGINT information for foreign intelligence and counterintelligence purposes ... In September 2001, NSA's compliance procedures defined *foreign communications as communications having at least one communicant outside the United States, communications entirely among foreign powers, or communications between a foreign power and officers or employees of a foreign power. All other communications were considered domestic communications. NSA was not authorized under E.O. 12333 to collect communications from a wire in the United States without a court order unless the communications originated and terminated outside the United States or met applicable exceptions to the requirement of a court order under FISA.*[118]
>
> In late September, [Michael] Hayden informed [George] Tenet[119] that he had expanded SIGINT[120] operations under E.O. 12333 authority.

> According to Hayden, Tenet later said that he had explained the NSA's expanded SIGINT operations to Vice President Cheney during a meeting at the White House. On 2 October 2001, Hayden briefed the House Permanent Select Committee on Intelligence on his decision to expand operations under E.O. 12333 and informed members of the Senate Select Committee on Intelligence by telephone.
> According to Hayden, Tenet told him that during the meeting the Vice President asked if the IC was doing everything possible to prevent another attack. The Vice President specifically asked Tenet if NSA could do more...Hayden told Tenet that nothing more could be done within existing authorities. In a follow-up telephone conversation, Tenet asked Hayden what the NSA could do if it was provided additional authorities. To formulate a response, Hayden met with NSA personnel, who were already working to fill intelligence gaps, to identify additional authorities to support SIGINT collection activities that would be operationally useful and technically feasible. In particular, *discussions focused on how NSA might bridge the "international gap," i.e., collection of international communications in which one communicant was within the United States....*
>
> After consulting with NSA personnel, he discussed with the White House how FISA constrained NSA collection of communications earned on a wire in the United States. Hayden explained that NSA could not collect from a wire in the United States, without a court order, content or metadata from communications that originated and/or terminated in the United States. *Hayden also said that communications metadata do not have the same level of constitutional protection as the content of communications and that access to metadata concerning communications having one end in the United States would significantly enhance NSA's analytic capabilities.* Hayden suggested that the ability to collect communications that originated or terminated in the United States without a court order would increase NSA's speed and agility. After two additional meetings with Vice President Cheney to discuss further how NSA collection capabilities could be expanded along the lines described at the White House meeting, the Vice President told Hayden to work out a solution with Counsel to the Vice President David Addington [emphasis added].[121]

Inspectors General Report on PSP Required by Congress

Title III of the Foreign Intelligence Surveillance Act of 1978

Amendments Act of 2008 (FISA Amendments Act)- signed into law on July

10, 2008 - required the Inspectors General of Intelligence Community agencies that participated in the PSP (the Inspectors General [IGs] of the DoD, DOJ, CIA, NSA, and ODNI; collectively, the "PSP IG Group") to conduct a comprehensive review of the program.

- *Why Did Congress Require the Report?* Before going on to some of the findings of unclassified partial version of the Report, it is worth remembering how Congress came to know (at least most of Congress and at least publicly) about the very secret President's Surveillance Program (or, after it was publicly exposed, the "Terrorist Surveillance Program"). The depth charges were two December 16, 2005 stories in the *New York Times*.[122,123]

  According to the *Times*, administration officials told the authors that the administration had briefed Congressional leaders about the program and notified the judge in charge of the Foreign Intelligence Surveillance Court. (See discussion of the briefings in the June 15, 2013, *Washington Post* story below.) According to the *Times*, government officials indicated that "over the past three years"[124] in an effort to track possible "dirty numbers" linked to Al Qaeda," the NSA had monitored without warrants the international telephone calls and international e-mail messages of hundreds - perhaps thousands - of people *inside* the United States [emphasis added]. The Agency,

> according to these officials, still sought warrants to monitor entirely domestic communications.
>
> As the *Times* noted, this previously undisclosed decision to permit some warrantless eavesdropping inside the country without court approval was a major shift in American intelligence-gathering practices, particularly for the NSA, whose mission is to spy on communications abroad. As a result, according to the authors, some officials familiar with the continuing operation questioned whether the surveillance had stretched, if not crossed, constitutional limits on legal searches: A former senior official who specializes in national security law said, "This is really a sea change. It's almost a mainstay of this country that the NSA only does foreign searches."[125]

One week later, Risen and Lichtblau revealed that the NSA had also been capturing American communications on a much broader scale by "tapping directly into some of the American telecommunication system's main arteries" with the cooperation of U.S. telecommunications companies.[126] As discussed below (under the discussion of Section 702), in 2013 (as a result of the Snowden revelations), the former was revealed as Upstream, and the latter was revealed as PRISM.

After the *New York Times* stories, President Bush admitted to a small aspect of the program - the monitoring of the communications of between 500 and 1000 people inside the United States with suspected connections to

Al Qaeda. As the EFF has detailed,[127] however, "other aspects of the Program were aimed not just at targeted individuals, but perhaps millions of innocent Americans never suspected of a crime."[128]

After a public outcry, the "Terrorist Surveillance Program" was technically terminated in 2007. The FISA Court and Congress ultimately ratified the program, however, and Congress amended FISA in 2007 (the Protect America Act) and 2008 (the FISA Amendments Act [FAA]) to grant the agency even broader data-gathering powers, under *Section 702* (discussed below).[129]

Two Versions: Unclassified and Partial, Declassified and Full[130]

The 43-page unclassified review report was released on July 10, 2009. As the *New York Times* reported at the time, however, "The bulk of the findings remain classified in separate reports from each of the five inspectors general, who represent the Justice Department, the N.S.A, the C.I.A., the Defense Department and the Office of National Intelligence."[131]

According to the unclassified version of the IGs' Report:

> The President authorized the NSA to undertake a number of new, highly classified intelligence activities. All of these activities were authorized in a single Presidential Authorization that was periodically reauthorized. The specific intelligence activities that were permitted by the Presidential Authorizations remain highly classified, except that beginning in December 2005 the President and other Administration officials acknowledged that these activities included the interception without a court order[132] of certain international communications where there is "a reasonable basis to conclude that one party to the communication is a member of al-Qa'ida, affiliated with al-Qa'ida, or a member of an organization affiliated with al-Qa'ida." The President and other Administration officials referred to this publicly disclosed activity as the "Terrorist Surveillance Program," a convention we follow in this

> unclassified report. We refer to other intelligence activities authorized under the Presidential Authorizations as the "Other Intelligence Activities.[133]

The specific details of the Other Intelligence Activities remain highly classified, although the Attorney General publicly acknowledged the existence of such activities in August 2007.[134] Together, the Terrorist Surveillance Program and the Other Intelligence Activities comprise the PSP.

The Presidential Authorizations were issued at intervals of approximately every 45 days.… [W]ith each reauthorization the CIA and later the NCTC prepared an assessment of current potential terrorist threats and a summary of intelligence gathered through the PSP and other means during the previous authorization period.… *Each of the Presidential Authorizations included a finding to the effect that an extraordinary emergency continued to exist, and that the circumstances "constitute an urgent and compelling governmental interest" justifying the activities being authorized without a court order.*

Although there was no legal requirement that the Authorizations be certified by the Attorney General or other Department of Justice official, current and former DOJ officials told us that this certification added value by *giving the program a sense of legitimacy*. Former Attorney General Gonzales stated that the NSA was being asked to do something it had not done before, and it was important to assure the NSA that the Attorney General had approved the legality of the program. He also stated that it was

important that the cooperating private sector personnel know that the Attorney General had approved the program. *In addition, Gonzales said that for "purely political considerations" the Attorney General's approval of the program would have value "prospectively" in the event of congressional or inspector general reviews of the program* [emphasis added].[135]

Attorney General Ashcroft gave his legal authorization to the program for the first two and a half years based on a "misimpression" of what activities the NSA was actually conducting.[136] In March 2004, a showdown occurred in Mr. Ashcroft's hospital room when top Justice Department officials refused to sign off on the legality of the program and threatened to resign. The report said that *the White House had the program continue by having Mr. Gonzales, then the White House counsel, sign the authorization* [emphasis added].[137]

The 747-page *fully declassified*[138] version was released on April 24, 2015, in response to a FOIA lawsuit brought by the *New York Times*.[139] The declassified version includes information about the Stellarwind (the code name for the President's Surveillance Program[140]) program: the NSA mining of information from email databases and gathered telephone metadata from the databases of cellphone service providers; and its gathering and analysis of the content of telephone conversations and email communications from these databases.

What We Learned as a Result of the Snowden Documents

A June 15, 2013 article in *The Washington Post* provides a good summary of some of what we learned from the Snowden documents. Primary among these is that "STELLARWIND was succeeded by four major lines of intelligence collection in the territorial United States, together capable of spanning the full range of modern telecommunications, according to the interviews and documents"[141]:

> Two of the four collection programs, one each for telephony and the Internet, process trillions of "metadata" records for storage and analysis in systems called MAINWAY and MARINA, respectively. Metadata includes highly revealing information about the times, places, devices and participants in electronic communication, but not its contents. The bulk collection of telephone call records from Verizon Business Services, disclosed this month by the British newspaper *Guardian*, is one source of raw intelligence for MAINWAY.
>
> The other two types of collection, which operate on a much smaller scale, are aimed at content. One of them intercepts telephone calls and routes the spoken words to a system called NUCLEON.
>
> For Internet content, the most important source collection is the PRISM project reported on June 6 by *The Washington Post* and *Guardian*. It draws from data held by Google, Yahoo, Microsoft and other Silicon Valley giants, collectively the richest depositories of personal information in history.

The article continued to give historical context to these disclosures:

> In the urgent aftermath of Sept. 11, 2001, with more attacks thought to be imminent, analysts wanted to use "contact chaining" techniques to build what the NSA describes as network graphs of people who represented potential threats.
>
> The legal challenge for the NSA was that its practice of collecting high volumes of data from digital links did not seem to meet even the relatively low requirements of Bush's authorization, which allowed collection of Internet metadata "for communications with at least one communicant outside the United States or for which no communicant

was known to be a citizen of the United States," the NSA inspector general's report said.[142]

Lawyers for the agency came up with an interpretation that said the NSA did not "acquire" the communications, a term with formal meaning in surveillance law, until analysts ran searches against it. The NSA could "obtain" metadata in bulk, they argued, without meeting the required standards for acquisition. [Jack] Goldsmith and [James] Comey did not buy that argument, and a high-ranking U.S. intelligence official said the NSA does not rely on it today, saying that as soon as surveillance data "touches us, we've got it, whatever verbs you choose to use. We're not saying there's a magic formula that lets us have it without having it."

When Comey finally ordered a stop to the program, Bush signed an order renewing it anyway. Comey, Goldsmith, FBI Director Robert S. Mueller III and most of the senior Bush appointees in the Justice Department began drafting letters of resignation. Then-NSA Director Michael V. Hayden was not among them.

According to the inspector general's classified report, Cheney's lawyer, [David] Addington, placed a phone call and "General Hayden had to decide whether NSA would execute the Authorization without the Attorney General's signature." He decided to go along.

The following morning, when Mueller told Bush that he and Comey intended to resign, the president reversed himself.

Three months later, on July 15, [2004,] the secret surveillance court allowed the NSA to resume bulk collection under the court's own authority. The opinion, which remains highly classified, was based on a provision of electronic surveillance law, known as "pen register, trap and trace," that was written to allow law enforcement officers to obtain the phone numbers of incoming and outgoing calls from a single telephone line.…

As for bulk collection of Internet metadata, the question that triggered the crisis of 2004, another official *said the NSA is no longer doing it. When pressed on that question, he said he was speaking only of collections under authority of the surveillance court.*[143]

"I'm not going to say we're not collecting any Internet metadata," he added. "*We're not using this program and these kinds of accesses to collect Internet metadata in bulk*" [emphases added].[144]

We will see, in the discussion of Section 702 later, that the program conducted under the FISC's authority is also implicated in the "incidental" collection of the content of USPs:

> When the NSA aims for foreign targets whose communications cross U.S. infrastructure, it expects to sweep in some American content "incidentally" or "inadvertently," which are terms of art in regulations governing the NSA. Contact chaining, because it extends to the contacts of contacts of targets, inevitably collects even more American data.…
>
> When asked why the NSA could not release an unclassified copy of its "minimization procedures," which are supposed to strip accidentally collected records of their identifying details, the official suggested a reporter submit a freedom-of-information request.[145]

Declassified Inspectors General Report

The 2013 disclosures by Snowden included a draft version of the NSA Inspector General's contribution to the 2009 43-page unclassified version.[146] It omitted discussion of many key facts that, then, were still classified. The government subsequently declassified many facts about surveillance.

The *New York Times* filed a FOIA lawsuit seeking release of the 747-page full and final report.[147] On April 24, 2015, in response to the lawsuit, the government fully declassified[148] the 2009 IG's Report.

- *Declassified 2011 Opinion of FISC Judge John D. Bates*[149]: In an 85-page October 2011 ruling (declassified and released post-Snowden), Judge Bates (then serving as chief judge on the Foreign Intelligence Surveillance Court) wrote that the court found that its approval, in March 2009, of a government presentation to justify the bulk collection

of all Americans' phone call records was "premised on a flawed depiction" of how the program operated and how the NSA uses the data and "buttressed by repeated inaccurate statements in the government's submissions" to the court.[150,151,152,153,154]

In a footnote, Bates wrote: "*This misperception by the FISC existed from the inception of its authorized collection in May 2006, buttressed by repeated inaccurate statements made in the government's submissions*, and despite a government-devised and court-mandated oversight regime" [emphasis added].[155]

The inaccurate statements were noted in a separate footnote, discussed below; they concerned revelations regarding the scope (volume and nature) of the NSA's acquisition of Internet transactions.

Misdirection by the NSA and the Department of Justice

It is evident in the Bates opinion that the NSA and the Department of Justice were as willing to misdirect the FISC as they were to misdirect Congress in the hearing before the House Judiciary Committee.[156,157] The Court's approval of contact chaining (hops) was based on "inaccurate statements made in the government's submissions." The approval was sought under the various permutations of the President's/Terrorist Surveillance Program.[158] When NSA Deputy Director John Chris Inglis, in his testimony before the House Judiciary Committee stated that *the FISA court*

"has approved us to go out two or three hops,"[159] and Deputy Attorney General James Cole said,

> The short court order...does not allow the government to access or use them. That is covered by another, more detailed court order [that]... provides that the government can only search the data if it has a reasonable, articulable suspicion that the phone number being searched is associated with certain terrorist organizations,[160]

they were referring to a 2007 Justice Department memo, discussed below.[161] In it, the Department of Defense (NSA) sought Attorney General approval pursuant to Executive Order 12333 of a proposed amendment to procedures governing the National Security Agency's Signals Intelligence Activities.[162]

2007 Justice Department Memo

The FISC ruling seems to point to a January 2007 announcement in which the Justice Department said it had worked out an "innovative" arrangement with the FISC that provided the "necessary speed and agility" to provide court review of all warrants on all wiretaps in terrorism investigations to monitor international communications of people inside the United States without jeopardizing national security.[163] What these terms meant was made clear at the announcement: A week prior, the Justice Department had obtained multiple orders or warrants (certifications) from the FISA court allowing it to monitor international communications in cases where there was probable cause to believe one of the participants was linked to Al Qaeda or an affiliated terrorist group.[164] According to then-Attorney

General Gonzales, "as a result of these orders any electronic surveillance that was occurring as part of the *Terrorist Surveillance Program* [emphasis added] will now be conducted subject to the approval of the Foreign Intelligence Surveillance Court."[165]

Permission to Gather and Analyze Metadata on U.S. Persons

Thanks to a Justice Department Memo, disclosed by Snowden, we know what the basis was for the "innovative arrangement." The NSA gained[166] authority to "analyze communications metadata associated with United States persons and persons believed to be in the United States," according to a November 20, 2007, Justice Department memo,[167] in which, as noted above, the Department of Defense (NSA) sought Attorney General approval *pursuant to Executive Order 12333* of a proposed amendment to procedures governing the National Security Agency's Signals Intelligence Activities [emphasis added].[168,169] The synopsis states that the "supplemental procedures"

> would clarify that the National Security Agency (NSA) may analyze communications metadata associated with United States persons and persons believed to be in the United States. These Supplemental Procedures would amend the existing procedures promulgated pursuant to Executive Order 12.333. That Order *requires the NSA to conduct its signals intelligence activities involving the collection, retention, or dissemination of information concerning United States persons in accordance with procedures approved by the Attorney General. Accordingly, changes to these procedures, such as those proposed here, also require your approval*. We conclude that the proposed Supplemental Procedures are consistent with applicable law and we recommend that you approve them [emphasis added].

> The communications metadata that the NSA wishes to []170 relates to telephone calls and electronic dialing, routing, addressing, and signaling information that does not concern the substance, purport, or meaning of the communication. … *This communications metadata has been obtained by various methods, including pursuant to the Foreign Intelligence Surveillance Act (FISA), 50 U.S.C. 1801*[171]*, et seq.,* [emphasis added] and resides in NSA databases. NSA plans to analyze this data primarily using a technique known as "contact chaining." Contact chaining involves the identification of telephone numbers, email addresses, or IP addresses that a targeted telephone number, IP address, or e-mail address has contacted or attempted to contact.[172]

In January 2008, Attorney General Michael B. Mukasey signed the document (including a set of "Supplemental Procedures" on the use of Americans' Internet metadata that had been signed in October 2007 by Secretary of Defense Robert Gates), stating:

> NSA will continue to disseminate the results of its contact chaining and other analysis of communications metadata in accordance with current procedures governing the dissemination of information concerning U.S. persons," without detailing the "current procedures."[173]

The Program Continues through the Obama Administration

This program continued for more than two years into the Obama administration.[174] In response to the release of the November 2007 Memo, the ACLU submitted a FOIA request to the DOJ in relation to the information presented in the 2007 announcement. (See below under Civil Society Engagement.)

- *FISA Court Opinion Granting the Application Made by the Government in 2006*: The Opinion of the FISC granting the Government's

application, made in the Government Memorandum of Law, was released by ODNI in November 2013.[175,176] The date of issuance of the Opinion is redacted, but it could well be the January 2007 certifications noted by Attorney General Gonzales above.

Civil Society Engagement

The 2013 release of the declassified 2011 FISC Opinion (above) marks the first time the government had disclosed a FISA court opinion in response to a Freedom of Information Act lawsuit, brought in 2012 by the Electronic Frontier Foundation. EFF sued after Sen. Ron Wyden (D-Ore.), in July 2012, got the Office of the Director of National Intelligence to acknowledge that the NSA's surveillance had at least once violated the Constitution.[177] Staff Attorney Mark Rumold said, "It's unfortunate it took a year of litigation and the most significant leak in American history to finally get them to release this opinion but I'm happy that the administration is beginning to take this debate seriously."[178]

ACLU submitted a FOIA request for the Government Memorandum of Law[179] (see above) submitted to the FISC on May 23, *2006,* by AG Alberto Gonzales, Steven G. Bradbury, Acting Assistant Attorney General, Office of Legal Counsel, and James Baker, Counsel for Intelligence Policy. ACLU received the document[180] on November 18, 2013. Civil liberties organizations also engaged in analysis[181] of what was known/learned about

the Program. As it was conducted entirely in secret until exposed - partially in 2009 and more fully in 2013 - there was little opportunity for advocacy other than reports and statements to congressional committees.

What Is Occurring Now?

This program is now incorporated into Section 702 of the 2008 FISA Amendments Act.

Section 702, Foreign Intelligence Surveillance Amendments Act

In 2008, Congress struck Section 702 of the FISA and replaced it with a new Section 702 created in Public Law 110-261, the 2008 FISA Amendments Act.[182,183] This version essentially codifies the President's Surveillance Program: It permits the bulk collection - from American companies - of Americans' overseas communications (telephone calls and e-mail, including the associated metadata) as long as the government is targeting foreigners abroad.[184] The section says surveillance may be authorized by the Attorney General and Director of National Intelligence without prior approval by the FISC, as long as minimization requirements and general procedures blessed by the court are followed. Rather than approving each target individually, the court simply approves *annual* "certifications" allowing the targeting of broad categories of people. It is, though, NSA agents who decide which particular phone lines and email accounts will be wiretapped, and there is no explicit requirement that these

particular phones and email addresses be foreign - only the *program*'s overall target must be.[185]

Although the targets of the eavesdropping have to be "reasonably believed" to be outside the United States, as former Deputy Attorney General David Kris explains in his book on the law,[186] the "target" of a surveillance program under FAA is typically just the foreign *group* - such as Al Qaeda or Wikileaks - that the government is seeking information *about*[187]:

> [The FAA's] certification provision states that the government under Section 1881a is "*not required to identify the specific facilities, places premises, or property at which an acquisition … will be directed or conducted*." This is a significant grant of authority, because it allows for authorized acquisition - surveillance or a search - directed at any facility or location. For example, an authorization targeting "al Qaeda" - which is a non-U.S. person located abroad—could allow the government to wiretap *any telephone that it believes will yield information from or about al Qaeda, either because the telephone is registered to a person whom the government believes is affiliated with al Qaeda, or because the government believes that the person communicates with others who are affiliated with al Qaeda, regardless of the location of the telephone*. … Review of the certification is limited to the question "whether [it] contains all the required elements"; the FISC does not look behind the government's assertions. Thus, for example, the FISC could not second-guess the government's foreign intelligence purpose of conducting the acquisition, as long as the certification in fact *asserts* such a purpose [emphasis added].[188]

Indeed, in a 2011 FISC Opinion - noted earlier and discussed in detail below - Judge John D. Bates found that the agency had violated the Constitution and noted serial misrepresentations to the Court.[189]

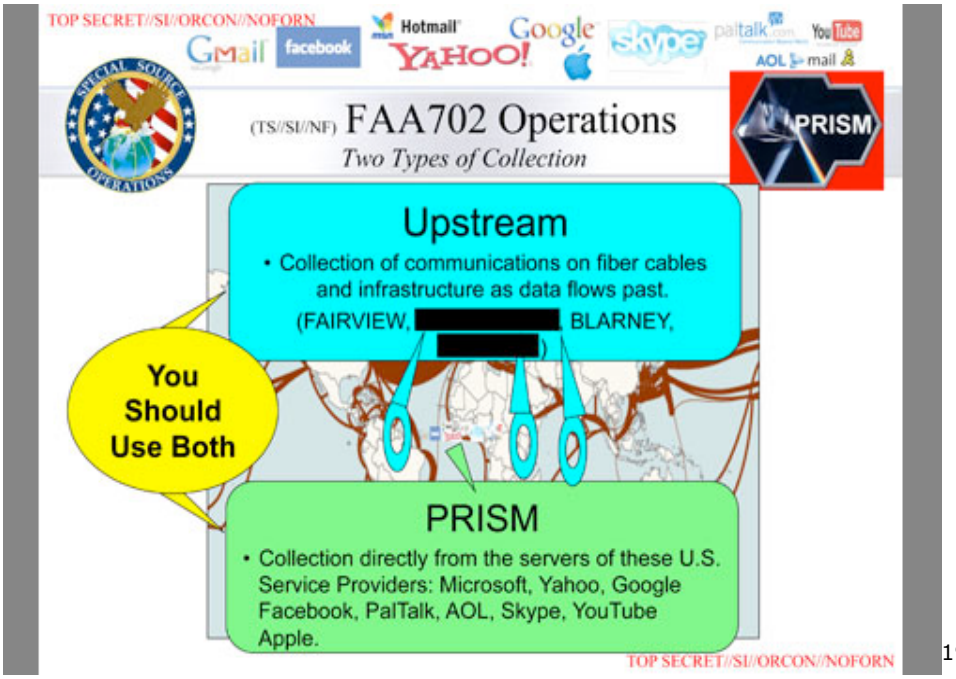
NSA Systemic Overcollection of Domestic Communications

On April 15, 2009, as a result of a disclosure from a non-identified source, the *New York Times* reported that the NSA is involved in "significant and systemic" overcollection of domestic communications.[190]

> The overcollection problems appear to have been uncovered as part of a twice-annual certification that the Justice Department and the director of national intelligence are required to give to the Foreign Intelligence Surveillance Court on the protocols that the N.S.A. is using in wiretapping. That review, which according to officials began in the waning days of the Bush administration and was continued by the Obama administration, led intelligence officials to realize that the NSA was improperly capturing information involving significant amounts of American traffic.
>
> Notified of the problems by the N.S.A., officials with both the House and Senate intelligence committees said they had concerns that the agency had ignored civil liberties safeguards built into last year's wiretapping law.[191]

And yet, as will be discussed below, officials with both the House and Senate intelligence committees reauthorized the legislation on January 11, 2018, without added protections for civil liberties.

What We Learned as a Result the Snowden Documents



[192]

Figure: Two Programs - PRISM and Upstream - Authorized By Section 702.

The PRISM program allows the NSA to receive data directly from the servers of U.S. companies like Microsoft, Yahoo, Skype, Google, and Facebook, and thus collect the contents of foreign targets' emails, text and video chats, photographs, and more.

The Upstream program was pointed to in the declassified Inspectors General Report and in a December 23, 2005, *New York Times* story, in which James Risen and Eric Lichtblau revealed that the NSA had been capturing American communications on a much broader scale by "tapping directly into some of the American telecommunication systems."[193] The program is discussed in detail below.

Declassified October 13, 2011, Opinion of FISC Judge John D. Bates

A 2011 Opinion (noted above) was released along with several others related to the collection program approved by Congress in 2008 under Section 702 of the FISA Amendments Act.[194,195] In the ruling, Judge Bates found that the agency had violated the Constitution and he noted serial misrepresentations to the Court[196]:

> The court is troubled that the government's revelations regarding N.S.A.'s acquisition of Internet transactions[197] mark the third instance in less than three years in which the government has disclosed a substantial misrepresentation regarding the scope of a major collection program.
>
> For the first time, the government has now advised the court that the volume and nature of the information it has been collecting is fundamentally different from what the court had been led to believe.[198]

Through Upstream, the NSA amasses a database of hundreds of millions of Americans' phone-call records: numbers dialed and the time and duration of calls (i.e., metadata), but no content. Bates continued: "Contrary to the government's repeated assurances, NSA had been routinely running queries of the metadata using querying terms that did not meet the required standard." The Court concluded that this requirement had been "so frequently and systematically violated that it can fairly be said that this critical element of the overall. . .regime has never functioned effectively."[199] Judge Bates further noted that the collection of purely domestic communications (Upstream) is likely to continue.

- *NSA collected tens of thousands of wholly domestic communications*: According to the opinion, the NSA, for several years, "has acquired, is acquiring, and if the certifications and procedures now before the Court is approved, will continue to acquire, unlawfully gathered tens of thousands of e-mails and other electronic communications between Americans as part of a now-revised collection method (see 2007 DOJ announcement and subsequent Memorandum discussed earlier). Based on NSA numbers the Court estimated that the spy agency may have been collecting as many as 56,000 "wholly domestic" communications each year.[200]

  Senator Ron Wyden, in a statement on August 21, 2013, said "The FISA Court has noted that this collection violates the spirit of the law but the government has failed to address this concern in the two years since this ruling was issued.[201] This ruling makes it clear that FISA Section 702, as written, is insufficient to adequately protect the civil liberties and privacy rights of law-abiding Americans and should be reformed."[202]

- *Upstream Collection Communications may contain entire Internet "Transactions" not related to the target and diverted into a repository:* Bates further noted that it was not until 2011 (the amended Section 702 was approved in 2008) that the NSA told the court that its "upstream" collection of Internet communications may contain *entire*

Internet "transactions" not related to the target (even as vaguely described the "target" might be) (reported by *The Washington Post* and others).[203,204] In June 2011, the NSA informed Bates that an Internet transaction may be a single communication, or it may include "multiple discrete communications," including those that are *not* to, from, *or about a target*. "That revelation fundamentally alters the Court's understanding of the scope of the collection conducted pursuant to Section 702," Bates said [emphasis added].[205]

Judge Bates' opinion also noted that under the NSA's "upstream" collection, the NSA diverted international data passing through fiber-optic cables in the United States into a repository where the material could be stored temporarily for processing, and for the selection of foreign communications, rather than domestic ones. According to a press conference call on the newly declassified court opinion, the Office of the Director of National Intelligence (ODNI) said that it was *"technologically impossible to"* filter out the "wholly domestic" communications between Americans.[206]

According to a report about a conference call (about the declassification and release of the ruling), an IC official indicated that the FISA Court paused the program (discussed below) but said,

> If you have a webmail email account, like Gmail or Hotmail, you know that if you open up your email program, you will get a screenshot of some number of emails that are sitting in your inbox. Those are all

transmitted across the internet as one communication. For technological reasons, the NSA was not capable of breaking those down, and still is not capable, of breaking those down into their individual [email] components.[207]

If one of those emails contained a reference to a foreign person believed to be outside the U.S. - in the subject line, the sender or the recipient, for instance - then the NSA would collect the entire screenshot "that's popping up on your screen at the time. On occasion, some of those [emails] might prove to be wholly domestic." If a foreign person being targeted is in contact with an American, "you can get all that U.S. person's screenshot" from his or her inbox.[208]

The official also noted, "The court found the NSA's procedures for purging wholly domestic communications needed to be beefed up, and that's what was done."[209]

- *Collection paused - then restarted:* In the Opinion, Judge Bates ordered the collection to stop until the NSA could propose an acceptable remedy. In November 2011, Bates signed an order approving the fix, which included a new technical means to segregate transactions *most likely* [emphasis added] to contain U.S. persons' communications, and reducing the retention period from five to two years. As discussed below, in April 2012 the NSA decided to conduct a purge of all upstream data collected since Section 702's inception in 2008.

- *Approved certification of targets*: As a result of Snowden releases, we learned that in July 2008, the court approved the first two certifications for "counterterrorism" and "foreign government" targets.[210] In March 2009, the court approved a third certification for targets engaged in the proliferation of weapons of mass destruction.[211] On their faces, these approvals seem unsurprising, but recall the explanation from former Deputy Attorney General David Kris about what the certification provision entails:

  > [The FAA's] certification provision states that the government under Section 1881a is "*not required to identify the specific facilities, places, premises, or property at which an acquisition … will be directed or conducted*." This is a significant grant of authority, because it allows for authorized acquisition—surveillance or a search—directed at any facility or location. For example, an authorization targeting "al Qaeda"—which is a non-U.S. person located abroad—could allow the government to wiretap *any telephone that it believes will yield information from or about al Qaeda, either because the telephone is registered to a person whom the government believes is affiliated with al Qaeda, or because the government believes that the person communicates with others who are affiliated with al Qaeda, regardless of the location of the telephone*. … Review of the certification is limited to the question "whether [it] contains all the required elements"; the FISC does not look behind the government's assertions. Thus, for example, the FISC could not second-guess the government's foreign intelligence purpose of conducting the acquisition, as long as the certification in fact *asserts* such a purpose [emphasis added].[212]

  This practice was codified in the 2012 reauthorization of the Act.[213]

What Has Occurred since the FISC Rulings?[214]

- *NSA Halts Collection of Americans' Emails "About" Foreign Targets*: On April 28, 2017, the NSA said it had halted collecting Americans' emails

and texts exchanged with people overseas that simply mention identifying terms- like email addresses - for foreigners on whom the agency is spying, but are neither to nor from those targets. NSA analysts are still, however, permitted to search for an American's information within another repository of emails gathered through the warrantless surveillance program's PRISM or "downstream" system, which gathers emails of foreign targets from providers like Gmail and Yahoo Mail. That system does not collect "about" communications. As noted below, the ruling from the FISC presiding judge, Judge Rosemary M. Collyer, subsequently authorized[215] the agency to use Americans' identifiers to query the *newly captured* [emphasis added] *upstream internet messages* for future intelligence investigations.

- *NSA Conducts Purge of All Upstream Collected 2008–2012*: In April 2012, the NSA decided to conduct a purge of all upstream data collected since Section 702's inception in 2008, senior intelligence officials said.[216] They could not estimate the quantity, but one official said it was "lots." According to another official: "It would have been everything."[217] But they have *continued to collect upstream data*.
- *"Backdoor Search Loophole" authorized by FISC*: An NSA official said the FISC's presiding judge, Judge Rosemary M. Collyer, authorized[218] the agency to use Americans' identifiers to query the *newly captured* [emphasis added] upstream internet messages for future intelligence

investigations. Once collected through PRISM, the communications of Americans are put into databases that are routinely searched by the FBI when starting - or even before officially starting - investigations into *domestic* crimes that may ultimately have nothing to do with foreign intelligence issues. With Judge Collyer's authorization, the government is now allowed to conduct these searches on communications collected as part of its "upstream" collection as well.

In April 2017, the NSA issued a Statement indicating that:

> After considerable evaluation of the program and available technology, NSA has decided that its Section 702 foreign intelligence surveillance activities will no longer include any upstream internet communications that are solely "about" a foreign intelligence target. Instead, this surveillance will now be limited to only those communications that are directly "to" or "from" a foreign intelligence target. These changes are designed to retain the upstream collection that provides the greatest value to national security while reducing the likelihood that NSA will acquire communications of U.S. persons or others who are not in direct contact with one of the Agency's foreign intelligence targets.
>
> In addition, as part of this curtailment, NSA will delete the vast majority of previously acquired upstream internet communications as soon as practicable.[219]

Privacy and Civil Liberties Concerns about Backdoor Search

The concern for privacy advocates and civil libertarians is that the government (in particular, the FBI) is permitted to seek out the content of Americans' communications that have been swept up through Section 702 *without any suspicion of wrongdoing, let alone a warrant*. Civil liberties and

privacy advocates call this the "backdoor search loophole" and have wanted Congress to require the government to obtain a warrant to search for Americans' incidentally collected information within the warrantless surveillance repository.

Senator Ron Wyden, in particular, has been dogged in pushing the Director of National Intelligence (DNI) for transparency about an estimate of the number of Americans whose communications have been collected under Section 702.[220] Members of the House have also weighed in strongly.[221] DNI Coats, at his February 28, 2017 confirmation hearing, told Senator Wyden (and the Committee) that "I'm going to do everything I can to work with Admiral Rogers in NSA to get you that number." In June, Director Coats said providing the number is "infeasible."[222]

Civil Society Engagement

In 2008, the EFF filed a lawsuit, *Jewel v. National Security Agency,* challenging "upstream" surveillance (as well as other bulk collection activities) on behalf of AT&T customers whose communications and telephone records were collected by the NSA.[223] In 2016, the district court rejected the plaintiffs' Fourth Amendment arguments, but has not issued a ruling on their First Amendment claims, and the case is (as of this writing) in discovery.[224]

In addition to suing the government agencies involved in the domestic dragnet, *Jewel v. NSA* also targets the individuals responsible for creating

authorizing and implementing the illegal program including DIRNSA Keith Alexander and former Vice President Dick Cheney, Cheney's former chief of staff David Addington, former Attorney General and White House Counsel Alberto Gonzales, and other individuals who ordered or participated in the warrantless domestic surveillance.[225]

The Obama Administration Moves to Dismiss the Case

The Obama administration moved to dismiss *Jewel* in 2009, claiming that litigation over the wiretapping program would require the government to disclose privileged "state secrets," and that it was immune from suit. The court instead ruled that the case should be dismissed on standing grounds. In December of 2011, the 9th U.S. Circuit Court of Appeals ruled that Plaintiffs' allegations were sufficient to provide standing and Jewel could proceed in district court.

In July 2012, EFF moved to have the court declare that the FISA law applies instead of the state secrets privilege; in September 2012, the government renewed its "state secrets" claims, and the matter was heard by the federal district court in San Francisco on December 14, 2012. In July 2013, the court rejected the government's "state secrets" argument, ruling that any properly classified details can be litigated under the procedures of FISA.[226] The court did dismiss some of EFF's statutory claims, but the other

claims, including that the program violates the First Amendment of the Constitution, continue.[227]

A Challenge to "Upstream" Surveillance of Online Communications

In addition, Wikimedia, PEN American Center, and *The Nation*, among other organizations, filed a lawsuit challenging "upstream" surveillance of online communications, raising both First Amendment and Fourth Amendment arguments.[228] The *Wikimedia* plaintiffs claim that upstream surveillance impedes their journalism, advocacy, and publishing activities. The district court ruled against Wikimedia in 2015, and an appeal is pending before the Fourth Circuit.[229] The Reporters Committee for Freedom of the Press filed an amicus brief in that case on behalf of itself and 17 news media organizations, arguing that upstream surveillance chills newsgathering and violates the First and Fourth Amendments.[230]

The EFF filed a FOIA request in 2016 for FISC opinions related to Section 702. On June 13, 2017, the FISA Court released 18 redacted opinions regarding FISA Section 702.[231,232] Mark Rumold of EFF notes that

> The opinions show that, almost from the outset of the law in 2008, the intelligence community has overstepped the court-imposed legal restrictions on the operation of the surveillance. Most of the documents tell a story of the IC overstepping boundaries, getting reprimanded by the FISC, but nevertheless being allowed to continue and even expand surveillance under the law.[233]

Additionally, organizations have repeatedly challenged the constitutional and statutory basis of bulk surveillance. Civil society

organizations have actively worked to inform and educate Congress and the public about the issues and what should be done: commentaries, letters, and organization testimony by civil society are here.[234] A number of these relate specifically to the expected reauthorization of the legislation in 2017 (see below).

USA Freedom Act

I go into some detail here as, before the FISA Amendment Act Reauthorization, these were the latest commitments made by the Intelligence Community.[235] They were only imposed with the IC's tacit consent, but give a clear sense of the known end-runs and violations perpetrated by the IC since the passage of the USA PATRIOT Act in 2001 - and are focused on those publicly known violations. Indeed, the full name of the Act is "Uniting and Strengthening America by Fulfilling Rights and Ending Eavesdropping, Dragnet-Collection and Online Monitoring Act." It is quite specific in its requirements and prohibitions (as opposed to the 2017 Reauthorization discussed below).

Title I

Title I bans the extant system of bulk collection under Section 215 of the PATRIOT Act.

- Additionally, it stipulates that for call detail records, for pen registers and trap-and-trace, and for the FBI to issue the bulk collection of national security letters, the government must base the applications on a *"specific selection term"* - a term that "specifically identifies a person, account, address, or personal device" in a way that "limit[s], to the greatest extent reasonably practicable, the scope of tangible things sought consistent with the purpose for seeking the tangible things."
- In regard to hops, the government can apply for records within the first hop of the specific selection term if it (1) states "reasonable grounds to believe that the call detail records sought to be produced based on [a] specific selection term ... are relevant to [an authorized] investigation," and (2) has "a reasonable, articulable suspicion" that the selection term is "associated with a foreign power engaged in international terrorism or activities in preparation therefor, or an agent of a foreign power engaged in international terrorism or activities in preparation therefor." To apply for records within the second hop, the government must state "session-identifying information or a telephone calling card number identified by the specific selection term" used to produce call detail records within the first hop.
- To safeguard against overbroad collection, the government must "*adopt minimization procedures*" calling for "the prompt destruction of

> all call detail records" determined not to be "foreign intelligence information." FISA court judges may, moreover, "impose additional, particularized minimization procedures" with respect to any "nonpublicly available information concerning unconsenting United States person."

Title III

Title III prohibits the use, in court proceedings, of information obtained under Section 702 through procedures deemed by a FISA Court to be "deficient concerning any United States person." Nor may the government "use...or disclose...in any other manner" such information. The law also addresses reform of the FISA Court. It provides for the appointment of amici curiae to assist the FISA Court, who may provide assistance with respect to "legal arguments or information regarding any … area relevant to the issue presented to the court," *but only if the FISA Court deems such information relevant and only in certain matters that "present a novel or significant interpretation of the law" in the eyes of the FISA Court* [emphasis added]. It also provides for limited appellate review of FISA Court decisions, as well as limited Supreme Court review of FISA Court of Review decisions.

The law requires the DNI to perform declassification *review* [emphasis added] of FISA Court opinions that "include...a significant construction or

interpretation" of any provision of law and, following such declassification review, make certain parts of FISA Court opinion publicly available.[236]

Title VI

Title VI prescribes extensive disclosure requirements with respect to data about FISA collection, in particular, under Sections 601 and 602, the government must disclose to Congress, as well as to the public, various items regarding the number of orders and certifications sought and received; *estimates of the number of people targeted and affected by surveillance*; and the number of appointments of amici curiae, among other items of information [emphasis added].

As noted earlier, USAF reinstates three provisions of the USA PATRIOT Act, which expired on June 1: roving wiretaps of terror suspects who change devices, surveillance of "lone wolf" suspects who are not affiliated with a terrorist organization, and the seeking of court orders to search business records.

As noted above, this law has the Intelligence Community's tacit imprimatur, so the limitations the law imposes should be read with an ear toward how they are likely to be interpreted.[237] What appear to be substantive interpretations appear in the reauthorization of the FISA Amendment Act below.

Civil Society Engagement

Civil society letters and testimony to Congress, from 2014 to 2015, on the USA FREEDOM Act are here.[238] As noted above, Title IV of the USA Freedom Act requires the DNI to perform declassification *review* of FISA Court opinions that "include...a significant construction or interpretation" of any provision of law and, following such declassification review, make certain parts of FISA Court opinion publicly available. In October 2016, the ACLU and Yale Law School's Media Freedom and Information Access (MFIA) filed a third motion seeking the release of all FISC opinions containing "novel or significant interpretations" of law issued between 9/11 and the passage of the USA Freedom Act in June 2015.[239]

FISA Amendment Act Reauthorization

The FISA Amendment Act was reauthorized in 2012 for five years.

- *Lead Up to 2017 Reauthorization*: The FISA Amendment Act was scheduled to expire on December 31, 2017. The intent of some segments of Congress was to reauthorize with no changes. Among some Members (including Senators and Representatives) and among civil society, an effort was made to reform the Act (the final iteration of this effort was the USA RIGHTS Act[240]). Specifically, the battle was over the NSA's "incidental" eavesdropping on Americans via its warrantless surveillance program, Upstream and the authorization for

the FBI to seek this data without a warrant. As discussed above, privacy and civil liberties advocates wanted this "backdoor search loophole" closed. They consider it a violation of the Fourth Amendment.

- *What Happened in the Reauthorization?* The Brennan Center for Justice made available in the days leading up to the votes on reauthorization a table[241] outlining the key issues (from the civil liberties and privacy perspectives, in italics). The key points of comparison of the USA RIGHTS Amendment" and the FISA Reauthorization Amendments Act (S.139)[242] are below. The discussion of *S. 139* also draws on the Center for Democracy and Technology (CDT) analysis of what the final bill contains.[243]

- *Prohibition of "about" collection (collecting communications not just to or from foreign targets, but also communications that merely reference them):*

  USA RIGHTS Amendment would have clarified that the government may not collect communications that are not to or from the target of surveillance.
  S. 139 codifies a permissive process for resuming "about" collection, where the NSA searches the content of communications for a targeted email address, phone number or other selector.

  As discussed earlier, "about" collection was not legislatively authorized, rather it was carried out under certifications from the FISC - although for a number of years it was not clear to the Court that

these collections were contained in the declarations made in the requests for certification. Upon understanding that "about" collection is more likely to return communications that are wholly unrelated to a "target" and purely domestic, the FISA Court instituted special privacy rules governing its use. When the NSA was unable to follow those rules, the practice stopped, with the possibility of resuming after court approval later.[244] The bill simply codified existing practice - if the NSA gets its compliance act together and the FISA Court signs off, the "about" program may start again. The bill adds a 30-day notice requirement to Congress so it may intervene and theoretically prevent its resumption.

The administration was set to obtain its next annual court order in late April 2018, which is a logical restart point if the technical issues are resolved.

- *Protection of Americans' privacy by requiring a warrant to access Americans' phone calls and e-mails:*

  S.139 authorizes such warrantless searches - a practice that was not previously expressly authorized in law - except in "predicated criminal investigations" unrelated to national security or foreign intelligence. A "predicated" investigation is one that has reached a certain stage of fact-finding.

  The government remains free under *S. 139* to conduct warrantless searches during the earlier phases of the investigation - which is when

backdoor searches routinely occur, according to the Privacy and Civil Liberties Oversight Board. In practice, a warrant would almost never be necessary, as the FBI itself has acknowledged. It has explained that it regularly searches its 702 databases with Americans' identifiers, looking for their communications only on the basis of a tip and long before formal investigations are opened.[245]

USA RIGHTS Amendment would have required the government to obtain a warrant before querying Section 702 data to obtain Americans' communications, with narrow exceptions—including an emergency exception that allows the government to proceed without a warrant if someone's life or safety is in danger (for instance, a kidnapping situation).

- *Prohibition on the government from collecting wholly domestic communications (namely, those with Americans on both ends of the call or e-mail) under Section 702:*

  S.139 does nothing to halt this practice.

  Recent exchanges between Senator Wyden and intelligence officials strongly suggest that the government is knowingly collecting wholly domestic communications under Section 702.[246]

  USA RIGHTS Amendment would have clarified that the government may not acquire communications it knows to be wholly domestic under Section 702.

- *Meaningful limitation on the ways in which Section 702 communications can be used against Americans:*

S. 139 contains no limits on the use of Americans' communications in investigations, or in legal proceedings other than criminal prosecutions (such as immigration actions). It also allows the use of Americans' communications as evidence in criminal cases if the Attorney General makes a determination - which cannot be challenged or reviewed by any court - that the case relates to or affects national security, or that it involves death, kidnapping, serious bodily injury, specified offenses against minors, critical infrastructure, cybersecurity, transnational crime, or human trafficking.[247]

USA RIGHTS Amendment would have limited the use of Americans' communications to cases involving terrorism, espionage, WMDs, cybersecurity threats, critical infrastructure, and threats against U.S. or allied armed forces, and prevent the use of warrantless access to evidence against Americans in ordinary criminal cases.

- *Ensure that people will be notified if the government uses Section 702-derived information against them in domestic legal proceedings; allow Americans who have reason to think their communications were obtained under Section 702 to challenge the surveillance*[248]:

  S.139, Section 111 requires the Attorney General to brief the Intelligence and Judiciary Committees on whether and how the Department of Justice notifies people that 702 information and other information collected under FISA authorities is used against them in official proceedings. This includes the introduction of 702 evidence in a criminal prosecution - but also in all trials, hearings, and proceedings, conducted by any "court, department, officer, agency, regulatory body." The notice requirements extend to any "aggrieved person" which includes Americans and non-citizens, as well as targets of surveillance and those who communicate with a target.

  The briefing required in Section 111 is critical, because the government has refused to explain how information derived from 702 surveillance is used to build cases, or is used to collect the same or similar information through other surveillance authorities, and thus

obscure the source of the information - known as "parallel construction." Regrettably, none of this has to be memorialized in writing, and none of it has to be made public.

USA RIGHTS Amendment would have clarified that the government must notify parties to legal proceedings when it uses information against them that it would not have acquired without Section 702 surveillance.

Also, codification in *S. 139* of a definition of "about" collection (see above) effectively removed any prospect of a statutory challenge based on a claim that "about" collection was not authorized by Congress.[249]

USA RIGHTS Amendment would have clarified that someone has been "injured" by Section 702 surveillance, for purposes of bringing allowed to bring a court challenge, if they reasonably believe their communications have been collected and if they have taken objectively reasonable steps to avoid the surveillance.

- *Number of known U.S. Persons for whom the FBI Searches/Number of queries FBI conducts:*

  S.139, Section 112 requires the Justice Department Inspector General (IG) to audit the process by which the FBI queries U.S. person information and uses it. The audit will include how the FBI handles searches for people whose nationality is not known, how the FBI ensures compliance with its internal querying procedures, and how the FBI uses queries in foreign intelligence investigations or criminal assessments. It also directs the IG to examine what is preventing the FBI from estimating the number of queries it conducts or the known U.S. persons for which it searches.

  The FBI has declined, thus far, to track this number.[250]

Some Whistleblower Protections

Additionally, Section 110 extends some whistleblower protections to IC contractor employees - about one-fourth of the IC workforce - the same incentives and protections as employees to blow the whistle on waste, fraud, or abuse without fear of retaliation. Employees have protection under President Obama's 2012 Presidential Policy Directive 19, Part A.[251] Under Section 110, contract employees are now protected to report wrongdoing, but enforcement mechanisms against retaliation are lacking in the bill itself: "The President shall provide for the enforcement of this subsection."

Civil Society Engagement

Since early 2016, civil society organizations have been writing letters to Congress, providing testimony, and posting commentaries[252] on the issues with Section 702 and how/why it needed - and needs - to be reformed

Issues with Congressional Oversight

It is obvious that something is deeply amiss with congressional oversight of the IC and its activities. This failure of robust oversight is critical, especially as the Administration White Paper claimed that the Section 215 bulk collection is legal, in large part because Congress twice (as

of August 2013) extended the PATRIOT Act without changing the terms of Section 215:

> Moreover, information concerning the use of Section 215 to collect telephony metadata in bulk was made available to all Members of Congress, and Congress reauthorized Section 215 without change after this information was provided. It is significant to the legal analysis of the statute that Congress was on notice of this activity and of the source of its legal authority when the statute was reauthorized.[253]

A key part of the argument that the use of Section 215 is legal rests on the Administration's claim that it gave notice to Congress about the expansion of the program. It is (sort of) hard to know whether to be as cynical about this issue as the authors of a Lawfare blog,

> Many members of Congress have spent the last few months appearing shocked by information leaked about the NSA's surveillance programs. The documents released yesterday, however, make clear that any member of Congress who did not know what was going on with respect to Section 702 surveillance did not *choose* to know - including with regard to the government's 2011 setback before the FISA Court.[254]

Or, to believe the avowals of lack of knowledge by some members of Congress.[255]

Limited Congressional Access to Intelligence Briefings

It is hard to argue, however, that Congress has not caved to the demands of the executive branch that only a very small handful of Members (Senators and Representatives) be allowed in on secret briefings to read secret documents - without members of their staffs who are experts on

these laws and might be able to ask challenging questions. The Members cannot take notes and cannot speak of what they read or heard. Rather than conduct oversight, the Congress has accepted the secret assurances of secret agencies about deeply secret programs, and has amended the law to expand the authority of the executive well beyond what even the USA PATRIOT Act did, at least up to the USA Freedom Act in 2015.

The New York Times reported on December 16, 2005, that after "the special program" started, congressional leaders from both political parties, including the chairmen and ranking members of the Senate and House intelligence committees, were brought to Vice President Dick Cheney's office in the White House.[256,257] The article noted that it was not clear how much the members of Congress were told about the presidential order and the eavesdropping program. Some of them declined to comment about the matter, while others did not return phone calls. Later briefings were held for members of Congress as they assumed leadership roles on the intelligence committees, officials familiar with the program said.

Senator Rockefeller's Concerns regarding Expanded Surveillance

After a July 2003 briefing, Senator Rockefeller, the West Virginia Democrat who became vice chairman of the Senate Intelligence Committee that year, sent a hand-written letter to Mr. Cheney expressing concerns

about the program.[258] On December 20, 2005, *The Washington Post* wrote that

> what he heard alarmed him so much that immediately afterward he wrote two identical letters, by hand, expressing his concerns. He sent one to Vice President Cheney and placed the other - as he pointedly warned Cheney he would - in a safe in case anyone in the future might challenge his version of what happened. Rockefeller proved prophetic. Yesterday the 21-year Senate veteran from West Virginia released his copy of the letter - which when written, was so sensitive he dared not allow a staffer to read it, let alone type it.
>
> In eight sentences on two sheets of Senate letterhead, Rockefeller wrote obliquely of "the sensitive intelligence issues we discussed today." Yesterday, after confirming with White House officials that the letter contains no classified information, the senator said the briefing's topic was the National Security Agency's expanded surveillance of Americans, publicly disclosed last week by the New York Times and now at the center of a political furor.[259]

There also has appeared to be a difference in how availability of information about the programs has been handled recently in the Senate and the House.[260] In 2013, according to *The Washington Post*,

> a declassified document - cited repeatedly by both Administration officials and congressional leaders as assurance of meaningful congressional oversight of the bulk collection of domestic telephone data - was withheld from circulation by the House Intelligence Committee. A cover letter to the House and Senate intelligence committees asked the leaders of each panel to share the written material with all members of Congress. The Senate Intelligence Committee did so. The House Committee opted, instead, to invite all 435 House members to attend classified briefings where the program was discussed - briefings that critics say were vague and uninformative. Justin Amash, the Michigan Republican who led the effort to defund the NSA's mass phone-records collection, said confronting intelligence officials during the briefings was "like a game of 20 questions," and added: "If you don't know about the program, you don't know what to ask about."[261]

- *The Intelligence Committees and E.O. 12333*: The National Security Act of 1947 requires that Congress be kept "fully and currently informed" about "significant" intelligence activities. Congress has arguably not been kept so informed, even though E.O.12333 activities are certainly "significant." The problem, legal experts and lawmakers have said, is that only the executive branch - and the intelligence agencies that are part of it - determines what "fully and currently informed" means and what details it needs to share with Congress. As reported in a 2013 article, House Intelligence Committee member[262] Adam Schiff, D-CA, noted, "There's no clear definition. We need to have a bigger discussion of what our mutual understanding is of what we want to be informed of."[263]

  The article also notes that Senator Dianne Feinstein, D-CA, who then chaired the Senate Intelligence Committee, has consistently defended the NSA's collection of domestic cellphone metadata, saying the program under which it is doing so is overseen by both the courts and Congress. At the time, she called for a broad review of what's taking place under 12333, noting that the order authorizes phone and email metadata collection beyond what FISA does. However, she also has said: "The other programs [the 12333 programs] do not (have the same oversight as FISA). And that's what we need to take a look at."[264] She indicated that her committee [Senate Select Committee on

Intelligence] has not been able to "sufficiently" oversee the programs run under the executive order: "Twelve-triple-three programs are under the executive branch entirely."[265]

- *Recent Efforts within Congress*: On March 22, 2016, eight members of the House Intelligence Committee sent a letter to the Chair and Ranking Member of the House Appropriations Committee, requesting adequate funding to the House Office of the Sergeant at Arms to support Top Secret Sensitive Compartmented Information Security (TS/SCI) Clearance investigations for individual designees from each House Permanent Select Committee on Intelligence Member's personal staff to support their Member for hearings and markups.[266] They noted:

  > The lack of funding places an onerous burden on individual Members, as they are unable to have the assistance of staff at the most crucial times, and is a major oversight considering their counterparts on the U.S. Senate Select Committee on Intelligence are afforded SCI Clearance investigations for personal office designees.[267]

  The House Intelligence Committee and its Senate counterpart were intended to consolidate review of intelligence matters, inform the entire Congress of intelligence activities, and hold public hearings to inform the broader public.

Civil Society Engagement

In September 2016, 33 organizations across the political spectrum sent a letter to Speaker of the House Paul Ryan and Democratic Leader Nancy Pelosi, urging them to adopt reforms to modernize the House's intelligence oversight in order to provide a meaningful check on the Executive Branch and reform how it conducts oversight over intelligence matters.[268]

The letter also urged them to consider establishing a distinct, broad-based review of the activities of the IC since 9/11, modeled after the 9/11 Commission or the U.S. Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities. As the letter notes, when questions were raised about the activities of the intelligence community in the 1970s,

> Congress reacted by forming two special committees, colloquially known as the Pike and Church committees. Reports preceded wholesale reforms of the intelligence community, including improving congressional-oversight mechanisms.[269] The outcome improved congressional oversight and the perception of its efficacy. The House should provide the new select committee adequate staffing and financial support, and give it a broad mandate to review practices and structures associated with congressional oversight of intelligence matters.[270]

The academic non-government community has also contributed analysis, commentary, and recommendations for remediation. A few of the contributions include those from Heidi Kitrosser[271] and Kathleen Clark.[272]

Funneling Requirements and the Separation of Powers

Kitrosser's article on information funnels in the sharing of executive branch information with Congress identifies key questions over whether funneling requirements infringe on the separation of powers and thus need not always be obeyed, what if anything should follow from information funneling - whether, for example, those with whom information is shared should be able to take some action in response to what they learn. Kitrosser uses the recent controversy about warrantless surveillance by the NSA as a jumping-off point to explore these questions, explains that Congress has the constitutional authority to set information-sharing requirements between the executive branch and itself, and suggests some answers to the questions as to how information funneling requirements should work.

Clark's article on *Congress' Right to Counsel* notes that, for decades, congressional leaders have acquiesced in the executive branch's insistence that certain intelligence information not be shared with congressional staffers, even those staffers who have high-level security clearances. As a result, Congress has been hobbled in its ability to understand and analyze key executive branch programs. It puts this issue into the larger context of Congress's right to access national security–related information, discusses congressional mechanisms for protecting the confidentiality of that information, identifies several constitutional arguments for Congress's right

to share information with its lawyers and other expert staff, and explores ways to achieve this reform.

Secrecy and the Foreign Intelligence Surveillance Court and Opinions

The United States Foreign Intelligence Surveillance Court (FISC) was established by Congress and authorized under the Foreign Intelligence Surveillance Act of 1978 or FISA.[273] Only the Executive Branch can submit requests. No one outside government can appear before the FISC judge without specific invitation.[274] Its rulings and its opinions are all secret.

The FISC started out (and has continued) as a secret court and, as Eric Lichtblau has noted, has quietly become almost a parallel Supreme Court, serving as the ultimate arbiter on surveillance issues and delivering opinions that will most likely shape intelligence practices for years to come, according to current and former officials familiar with the court's classified decisions.[275]

The FISC, whose statutory role is to approve warrant applications for surveillance activities related to national security, seems to have operated for years prior to 9/11 in the manner Congress had intended. Recent revelations raise significant questions about the conduct of the court. Instead of approving warrant applications, FISA court judges are, as noted earlier in regard to Section 215 orders, reviewing and approving bulk collections and "programmatic surveillance."

The Extended Authority of the FISC

Perhaps the greatest change at the FISC is that judges are no longer simply reviewing warrant applications for individual surveillance operations. The authority of the Court has been extended since 2001. It now has the authority to permit the electronic surveillance of entire categories—"without the need for a court order for each individual target" - of non-USPs located abroad.[276] Under this provision, instead of issuing individual court orders, the FISC approves annual certifications submitted by the Attorney General and the DNI that identify categories of foreign intelligence targets.[277] But although the statutes passed by Congress are available to the public, how those statutes have been interpreted and used remains secret.

Civil society (and others) talk about "capture," most frequently referring to the capture of regulatory agencies by outside (non-governmental) "interests." It is not inappropriate to talk about the FISC being captured by the White House and the IC. As noted above, we have seen some faint glimmerings of push-back (particularly in the House) in Congress.

Some FISC Orders and Opinions Declassified in Response to FOIA Litigation

On September 5, 2013, in a court filing[278] responding to a judge's order - in response to EFF FOIA litigation - the Justice Department said that

they would make public a host of material that will "total hundreds of pages" by next week, including:

> orders and opinions of the FISC issued from January 1, 2004, to June 6, 2011, that contain a significant legal interpretation of the government's authority or use of its authority under Section 215; and responsive "significant documents, procedures, or legal analyses incorporated into FISC opinions or orders and treated as binding by the Department of Justice or the National Security Agency."[279]

The U.S. government says it is "broadly construing" that order and is declassifying a larger set of documents than the ruling requires.[280] It provided hundreds of pages of documents to the Electronic Frontier Foundation in response to a lawsuit under the Freedom of Information Act.[281]

Some Recommendations for Reform of FISC

The academic non-government community has also contributed analysis, commentary, and recommendations for remediation in this area. A few of the contributions include those from Emily Berman and Robert Stein, Walter Mondale, and Caitlinrose Fisher.[282,283]

Berman's article, *The Two Faces of the Foreign Intelligence Surveillance Court*, argues that after the Snowden disclosures, U.S. surveillance activities were thrust to the forefront of public debate, including questions about the Foreign Intelligence Surveillance Court ("FISA Court"). The discussion, however, has underemphasized a critical feature of the way the FISA Court works: Not only its traditional role of "gatekeeper," but also

the additional - and entirely different - role of "rule maker." Further, the Article provides an assessment of the attempt to reform the FISA Court in the recently enacted USA FREEDOM Act of 2015. She concludes that the Act represents a missed opportunity: In not fully appreciating or accounting for the unique challenges that the court's rule-making function poses, the Act does not nearly go far enough in bolstering the court's rulemaking competence. Moreover, she argues the Act neglects (as has the public debate) a critical area for reform: ensuring sufficient flow of information from the Executive Branch to the FISA Court. The article explores the nature of this challenge and offers some additional reform ideas for consideration.

Stein, Mondale, and Fisher note that in the wake of 9/11, Congress significantly altered FISA's scheme, opening the door once again to executive overreach. Due to the changes to FISA, the Executive Branch is able to engage in practices similar to those that catalyzed the formation of the Church Committee and the enactment of FISA. This article chronicles the evolution of FISA and the FISA Court. Drawing on the unique perspective of Vice President Mondale, the article analyzes the ways in which the post-9/11 Act and the Court are at odds with their original design.[284] The article argues that such overreach is possible in part because of structural changes to the FISA Court and the executive branch's invocation of the need for secrecy in non-FISA Court proceedings. According to the authors, the recently enacted USA FREEDOM Act fails to fix the structural issues that currently limit the

authority and efficacy of the FISA Court. The FISA Court no longer serves its intended function as a specialized Article III court of limited jurisdiction; rather, it is more akin to an adjunct to the executive branch, lending legitimacy to intelligence operations without practically limiting executive authority. The article concludes by recommending tangible actions Congress can and should take - structures and processes that limit executive authority and comport with Article III of the United States Constitution.

Intelligence Community Transparency Since Snowden

The two epigraphs I included at the start of this article point to the critical question that bookends it and is at its heart: *Why would or should we trust the Intelligence Community?* Is there a true change of heart and mind reflected in the second quote from Bob Litt, or is the first one the truth and the second one public relations?

As I have laid out in the pages above, the White House, the Department of Justice, and the NSA have repeatedly lied (at a minimum, misdirected and "misrepresented") to the FISC, to Congress, and - not least- to the American public. It is noteworthy that, since 2013, the NSA, the CIA, and the ODNI have each created an Office of Civil Liberties, Privacy, and Transparency, the heads and staffs of which are open, take their roles and responsibilities seriously, and have shown themselves to be trustworthy. The concerns expressed here are not intended to malign them or cast aspersions.

Members of the privacy, civil liberties, and government openness communities have held "Chatham House Rule" meetings with these and other representatives from ODNI and NSA on the issue of declassification of FISC opinions and the government's unwillingness to provide an index of any sort of those opinions it declines to declassify and release.[285]

Members of these communities have also met with these and other representatives from ODNI and the other intelligence agencies. Many of the discussions focused on transparency about an estimate of the number of Americans whose communications have been collected under Section 702. Although the civil society participants have offered ideas - in particular sampling - to counter the government's claim that they would have to invade the privacy of the individuals collected under 702, and that the numbers make it impractical, the NSA continues to resist. As noted earlier, DNI Coats has stated that this is "infeasible."

The ODNI has put a very large amount of information up on two sites.[286] As noted in a February 2015 article, though, "Tens of thousands of pages of records on those efforts have been made public, largely in response to Freedom of Information Act requests and lawsuits."[287] As noted at the beginning of this article, some of the postings since then seem voluntary.

In December 2017, the Chief of the ODNI Office of Civil Liberties, Privacy and Transparency, notified various organizations that

> in September 2017, his office posted a guide with links to certain officially released documents related to the use by the Intelligence

> Community (IC) of national security authorities. These documents have been published to meet legal requirements, as well as to carry out the Principles of Intelligence Transparency for the IC.... We have now updated that Guide[288] to include links to additional officially released documents. The updated links are annotated with an asterisk. In addition to this Updated Guide, please note that the IC has launched a new web portal, Intel.gov,[289] which features the "Intel Vault." The Intel Vault[290] enables users to conduct full-text searches of the Section 702 documents posted on IC on the Record.[291]

Lack of Whistleblower Protections within the Intelligence Community

There are some recent disturbing reports, however, reflecting on the IC's commitment to accountability. The first is a Daily Beast report on February 11, 2018, noting that, according to an April 2017 finding (of an inspection run out of the Intelligence Community Inspector General office), the spy agencies - including the CIA and the NSA - were failing to protect intelligence workers who report waste, fraud, abuse, or criminality up the chain of command.[292] The investigators working on the report looked into 190 cases of alleged reprisal in six agencies, and uncovered that "over and over and over again, intelligence inspectors ruled that the agency was in the right, and the whistleblowers were almost always wrong." According to the article, the report had been near completion but had been sequestered by the acting head of the Intelligence Community Inspector General office, Wayne Stone, following the discovery that one of the inspectors was himself a whistleblower in the middle of a federal lawsuit against the CIA (for retaliation for his own whistleblowing), according to former IC IG officials.

Destruction of Presidential Surveillance Program Data

A second report, from Politico, is that, according to recent court filings, the NSA destroyed surveillance data - Presidential Surveillance Program Internet content data - it pledged to preserve in connection with pending lawsuits, and apparently never took some of the steps it told a federal court it had taken to make sure the information wasn't destroyed[293]:

> Since 2007, the NSA has been under court orders to preserve data about certain of its surveillance efforts that came under legal attack following disclosures that President George W. Bush ordered warrantless wiretapping of international communications after the 2001 terrorist attacks on the U.S. In addition, the agency has made a series of representations in court over the years about how it is complying with its duties.
>
> However, the NSA told U.S. District Court Judge Jeffrey White in a filing on Thursday night and another little-noticed submission last year that the agency did not preserve the content of internet communications intercepted between 2001 and 2007 under the program Bush ordered. To make matters worse, backup tapes that might have mitigated the failure were erased in 2009, 2011 and 2016, the NSA said.
>
> "The NSA sincerely regrets its failure to prevent the deletion of this data," NSA's deputy director of capabilities, identified publicly as "Elizabeth B.," wrote in a declaration filed in October. "NSA senior management is fully aware of this failure, and the Agency is committed to taking swift action to respond to the loss of this data."
>
> In the update Thursday, another NSA official said the data were deleted during a broad, housecleaning effort aimed at making space for incoming information.
>
> The NSA's review to date reveals that this [Presidential Surveillance Program] Internet content data was not specifically targeted for deletion," wrote the official, identified as "Dr. Mark O," "but rather the PSP Internet content data matched criteria that were broadly used to delete data of a certain type…in response to mission requirements to free-up space and improve performance of the [redacted] back-up

> system. The NSA is still investigating how these deletions came about given the preservation obligations extant at the time. The NSA, however, has no reason to believe at this time that PSP Internet content data was specifically targeted for deletion.[294]

What Does the IC mean by "Transparency"?

Finally, though, a fundamental question is what the IC means by "transparency" and the reasons for their engaging in it. In his Introduction to the 3rd Annual SIGINT Progress Report, and his final missive as DNI, James Clapper wrote:

> I issued the Principles of Intelligence Transparency two years ago, and believe more strongly than ever that responsible transparency is becoming increasingly inseparable from public trust, and consequently, from mission success. We cannot accomplish our mission without public trust, and to earn and retain that trust, we must better explain both our role in protecting national security, and the rules and oversight framework that governs our activities. This includes engaging with the public to enhance their understanding of the IC—including meeting with civil society representatives to hear their concerns and better explain our perspectives. Of course, we must continue to carry out our obligation to protect intelligence sources, methods, and activities when disclosure would harm national security. Transparency is difficult, but also, in my view, essential.[295]

Belief in Accountability or Public Relations?

I asked above if the second of the two epigraphs (included at the start of this article) reflect a true change of heart and mind by Bob Litt, or is the first one the truth and the second one public relations? My suspicions are toward the latter. Every public-facing statement I have found from the intelligence agencies' leadership post-Snowden often uses exactly the same words and phrases.[296] Each also contextualizes the transparency

commitment, as does DNI Clapper's statement above, with a limitation (an implied or stated "but of course") - *an obligation to protect intelligence sources, methods, and activities*. This is facially unobjectionable, but there is no legal definition of "methods," so it is an open door to withholding information.[297]

The framing here, as in the second Bob Litt quote at the start of this paper, is that public trust is essential to mission success - not a value in itself. Transparency is protective, not a commitment to the public or to accountable government.

Keeping the Bubble of Secrecy Pierced

The reality is, of course, that the information is in the hands of the intelligence agencies that have understood their mission, as one individual put it, to be collecting information and keeping it secret, not sharing it. From the perspective of the public, and its representatives, however, "we don't know what we don't know." As James Madison famously said,

> A popular Government, without popular information, or the means of acquiring it, is but a Prologue to a Farce or a Tragedy; or, perhaps both. Knowledge will forever govern ignorance: And a people who mean to be their own Governors, must arm themselves with the power which knowledge gives.[298]

Public Responsibility

Our charge as the American public is to figure out how to wrest knowledge from the hands of our government. Our difficulty is identifying

how we can make Madison's cautionary advice real. It is, without doubt, an uphill and ongoing struggle, but the public is not on its own.

As has been amply demonstrated throughout this article (and in the endnotes), the press is a powerful ally in ferreting out lies and engaging in investigative truth-telling. Especially now, they need our financial as well as our rhetorical and moral support.

Members of the press are not alone in calling out illegal, abusive, and/or fraudulent government practices. Often, their information comes from individuals inside the government, sometimes - but not often - information the agency has *properly* classified.[299] Not everyone who works for the federal government has equivalent whistleblower protection, however; IC employees do, and IC contract employees now have some.[300] Indeed, a recent Senate Intelligence Committee report on the Intelligence Authorization Act for Fiscal Year 2018 stated:

> The Committee remains concerned about the level of protection afforded to whistleblowers within the IC and the level of insight congressional committees have into their disclosures. It is the Committee's expectation that all Offices of Inspector General across the IC will fully cooperate with the direction provided elsewhere in the bill to ensure both the Director of National Intelligence and the congressional committees have more complete awareness of the disclosures made to any IG about any National Intelligence Program funded activity.[301]

As noted above, the Section 702 Reauthorization, Section 110, extends some whistleblower protections to IC contractor employees, who are about one-fourth of the greater IC workforce.[302] Under Section 110, contract

employees are now protected to report wrongdoing, but enforcement mechanisms against retaliation are lacking in the bill itself: "The President shall provide for the enforcement of this subsection."

A Troubling Development

In a troubling, and at this writing still unresolved, development, the IC whistleblower ombudsman, Dan Meyer, was barred in October 2017 from communicating with whistleblowers, which is the main responsibility of his job as the Executive Director for Intelligence Community Whistleblowing and Source protection. The four-year-old program of outreach and training on proper disclosure and whistleblower protections for employees working with classified material is endangered. According to *Foreign Policy*:

> The intelligence community's central watchdog is in danger of crumbling thanks to mismanagement, bureaucratic battles, clashes among big personalities, and sidelining of whistleblower outreach and training efforts, sources told FP. A strong whistleblowing outlet is needed as an alternative to leaking, and to protect employees from retaliation for reporting misconduct, proponents of the office argue. But many intelligence officials see outreach to their employees as an attempt to cultivate leakers or outside interference, rather than a secure, proper way to report potential violations of law.[303]

The culture depicted here guarantees there will continue to be a need for organizations that vet the claims made by whistleblowers who are blocked and retaliated against internally, and work with them to get the identified problems appropriately addressed.[304]

Conclusion

As members of the public, we each have the responsibility to hold our Senators' and our Representative's respective feet to the fire. We have to be vigilant in meeting with them and in following them in the news - and not just their Twitter or Facebook feeds - to ascertain if they are working to protect both our First Amendment rights and our Fourth Amendment protections against the government, for example, "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."

This may seem a daunting task - and it is. A place to start is by looking to the experts who present testimony, send letters to Congress, and prepare analysis and commentaries.[305] Two online publications - Just Security and Lawfare - among others, provide ongoing coverage of the issues raised in this article, as do the journalists cited (although they may well have moved to other venues).[306,307] The problems have not gone away, and they are unlikely to do so in the foreseeable future.[308]

1 Director, Government Information Watch.
2 Any United States citizen or alien admitted for permanent residence in the United States, and any corporation, partnership, or other organization organized under the laws of the United States. *22 U.S. Code § 6010*, https://www.law.cornell.edu/uscode/text/22/6010.
3 Sari Horwitz and William Branigin, "Lawmakers of both parties voice doubts about NSA surveillance programs," *Washington Post*, July 17, 2013, https://www.washingtonpost.com/world/national-security/house-committee-holds-hearing-on-nsa-surveillance-programs/2013/07/17/ffc3056c-eee3-11e2-9008-61e94a7ea20d_story.html.
4 Robert S. Litt, *As Prepared for Delivery—Remarks of ODNI General Counsel Robert Litt at American University Washington College of Law Freedom of Information Day Celebration*, March 17, 2014, https://icontherecord.tumblr.com/post/79998577649/as-prepared-for-delivery-remarks-of-odni-general.
5 The House version of the USA Freedom discussed later.
6 Patrice McDermott, "One Year Later: Snowden Disclosures' Effect on Secret Laws," *RollCall*, June 4, 2014, http://www.rollcall.com/news/one_year_later_snowden_disclosures_effect_on_secret_laws_commentary-233569-1.html.
7 Civil Society Letters, Commentaries, and Testimony**.** See Warrantless Surveillance-Coalition letters, https://govinfowatch.dream.press/warrantless-surv…oalition-letters/; Organizational Testimony-Warrantless Surveillance, https://govinfowatch.dream.press/organizational-testimony-warrantless-surveillance/; and Section 702 Reauthorization Commentaries https://govinfowatch.net/section-702-reauthorization-commentaries/.
8 Although the President's Surveillance Program preceded the USA PATRIOT Act chronologically, it was not acknowledged publicly until 2005, and then only partially.
9 Seymour Hersh, "Huge C.I.A. Operation Reported in U.S. Against Antiwar Forces, Other Dissidents in Nixon Years," *New York Times,* December 22, 1974, http://www.nytimes.com/1974/12/22/archives/huge-cia-operation-reported-in-u-s-against-antiwar-forces-other.html.
10 United States Senate, Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities (The Church Committee)*,* April 29, 1976, https://www.senate.gov/artandhistory/history/common/investigations/ChurchCommittee.htm#Origins.
11 United States Senate, Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities, https://www.senate.gov/artandhistory/history/common/investigations/ChurchCommittee.htm.
12 Laura K. Donohue, "Anglo-American Privacy and Surveillance," *Journal of Criminal Law and Criminology* 96 no. 3 (March 2006): 1080-1081. *Operation* SHAMROCK began in World War II, when the military placed censors at RCA Global, ITT World Communications, and Western Union International. DOD told the companies to continue forwarding intercepts, assuring them that they would be exempt from criminal liability or public exposure as long as Truman remained in the White House. From 1949 until 1975 the project continued (from 1952 under the control of the National Security Agency) without the knowledge of subsequent Presidents. To keep the project under the radar, NSA deliberately refrained from formalizing the relationship in any sort of (traceable) document. By the 1970s, from the magnetic tapes that recorded all telegraph traffic, the NSA was selecting approximately 150,000 messages per month for its analysts to read and circulate. While Operation SHAMROCK represented a broad, information-gathering effort, NSA also undertook a project

[MINARET] that placed particular "individuals or organizations involved in civil disturbances, anti-war movements, [or] demonstrations" under surveillance. Project MINARET maintained a Top Secret classification, named agents only. The charter specified that although NSA instigated the project, it would not be identified with the operation.
13 Scott A. Boykin, "The Foreign Intelligence Surveillance Act and The Separation of Powers," *University of Arkansas at Little Rock Law Review* 38, no. 1 (2015): 33-62; https://lawrepository.ualr.edu/lawreview/vol38/iss1/2.
14 U.S. Congress, Senate, Select Committee To Study Governmental Operations, Intelligence Activities And The Rights Of Americans, 94 Cong., 2d sess., 1976, S. Rep. No. 94-755, at 10–13 (1976), *Book III, Supplementary Detailed Staff Reports on Intelligence Activities and the Rights of Americans*, https://www.intelligence.senate.gov/sites/default/files/94755_III.pdf.
15 U.S. Congress, Senate, Select Committee To Study Governmental Operations, Intelligence Activities And The Rights Of Americans. *Final Report, Book II, Intelligence Activities and the Rights of Americans, III; Book I, 287-339*. The recommendations cover an array of agencies and practices. See https://www.intelligence.senate.gov/sites/default/files/94755_II.pdf.
16 "Scope of Recommendation - The scope of our recommendations coincides with the scope of our investigation. We examined the FBI, which has been responsible for most domestic security investigations as well as foreign and military intelligence agencies, the IRS, and the Post Office, to the extent they became involved incidentally in domestic intelligence functions. The agencies whose activities are specifically covered by the recommendations are: (i) the Federal Bureau of Investigation; (ii) the Central Intelligence Agency; (iii) the National Security Agency and other intelligence agencies of the Department of Defense; (iv) the Internal Revenue Service; and (v) the United States Postal Service.
17 See *Senate Resolution 400*, *Congressional Record*, May 19, 1976, p. 14673**.** https://www.senate.gov/artandhistory/history/common/investigations/pdf/ChurchCommittee_SRes400_SSCI.pdf.
18 See U.S, Senate Select Committee on Intelligence, Overview of the Senate Select Committee on Intelligence Responsibilities and Activities, http://www.intelligence.senate.gov/about.html.
19 Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities, 1975-76 (Church Committee), https://www.intelligence.senate.gov/resources/intelligence-related-commissions.
20 See Note 2.
21 *Foreign Intelligence Surveillance Act of 1978*, Pub. L. 95-511, 92 Stat. 787, §§ 102(a)(1),101(h) (codified as amended at 50 U.S.C. §§ 1801(f)(1)–(4), 1802(a)(1)(A)(i)).
22 *Executive Order 12333 - United States Intelligence Activities***.** The provisions of Executive Order 12333 of Dec. 4, 1981, appear at 46 FR 59941, 3 CFR, 1981 Comp., p. 200, unless otherwise noted; see https://www.archives.gov/federal-register/codification/executive-order/12333.html.
23 National Security Agency/Central Security Service, "Signals Intelligence (SIGINT) is *intelligence* derived from electronic *signals* and systems used by foreign targets, such as communications systems, radars, and weapons systems." See https://www.nsa.gov/what-we-do/signals-intelligence/.
24 Ali Watkins*,* "Most of NSA's Data Collection Authorized by Order Ronald Reagan Issued,*"* *McClatchy DC Bureau*, November 21, 2013, http://www.mcclatchydc.com/news/nation-world/national/national-security/article24759289.html.
25 The President's Surveillance Program is defined in the FISA Amendments Act as the intelligence activity involving communications that was authorized by the President during the period beginning on 11 September 2001 and ending on 17 January 2007, including the

program referred to by the President in a radio address on 17 December 2005 (commonly known as the Terrorist Surveillance Program).
26 Scott A. Boykin, "The Foreign Intelligence Surveillance Act and The Separation of Powers."
27 The cover term NSA used to protect the President's Surveillance Program. See Offices of Inspectors General of the Department of Defense, Department of Justice, Central Intelligence Agency, National Security Agency, Office of the Director of National Intelligence, *Fully Declassified Version Report on the President's Surveillance Program, Report No. 2009-0013-AS*, FN 1, p. 1, 2009, https://oig.justice.gov/reports/2015/PSP-09-18-15-full.pdf.
28 Charlie Savage, "Government Releases Once-Secret Report on Post-9/11 Surveillance," *New York Times*, April 25, 2015, https://www.nytimes.com/interactive/2015/04/25/us/25stellarwind-ig-report.html.
29 Clearly, E.O. 12333 predates it.
30 Inspector General of the Department of Defense, *Unclassified Report on the President's Surveillance Program,* July 10, 2009, is the only IG Report included in *Unclassified Report on the President's Surveillance Program*, Prepared by the Offices of Inspectors General of the Department of Defense, Department of Justice, Central Intelligence Agency, National Security Agency, Office of the Director of National Intelligence, Report No. 2009-0013-AS, 2009, https://oig.justice.gov/special/s0907.pdf*;* also available at https://fas.org/irp/eprint/psp.pdf.
31 Offices of Inspectors General, *Unclassified Report on the President's Surveillance Program*, Report No. 2009-0013-AS.
32 See Note 2.
33 The PRISM program allows the NSA to receive data directly from the servers of U.S. companies like Microsoft, Yahoo, Skype, Google, and Facebook, and thus collect the contents of foreign targets' emails, text and video chats, photographs, and more.
34 In 2005, James Risen and Eric Lichtblau revealed the "Upstream" program in a *New York Times* article that the NSA had been capturing American communications on a much broader scale by "tapping directly into some of the American telecommunication systems."
35 James Risen and Eric Lichtblau, "Spy Agency Mined Vast Data Trove, Officials Report," *New York Times*, December 23, 2005, https://www.nytimes.com/2005/12/24/politics/spy-agency-mined-vast-data-trove-officials-report.html.
36 See note 24.
37 *Executive Order 12333 - United States Intelligence Activities*.
38 I draw much of this initial discussion, unless otherwise noted, from Ali Watkins, "Most of NSA's Data Collection Authorized by Order Ronald Reagan Issued."
39 See note 22.
40 The last one occurred under President Obama.
41 Ali Watkins, "Most of NSA's Data Collection Authorized by Order Ronald Reagan Issued."
42 National Security Agency/Central Security Service, *The National Security Agency: Missions, Authorities, Oversight and Partnerships*, August 9, 2013, https://www.nsa.gov/news-features/press-room/statements/2013-08-09-the-nsa-story.shtml.
43 Office of the Director of National Intelligence, *Intel.gov, Mission, Our Values, Accountability*, https://www.intelligence.gov/mission/our-values/343-accountability.
44 As noted above, drawn from Ali Watkins, "Most of NSA's Data Collection Authorized by Order Ronald Reagan Issued."
45 See Note 2.
46 With a warrant, as noted above, but it is not clear what entity issues such a warrant. It is likely a FISC warrant under Section 702 (discussed below).

47 John Napier Tye, "Meet Executive Order 12333: The Reagan rule that lets the NSA spy on Americans," *Washington Post*, July 18, 2014, https://www.washingtonpost.com/opinions/meet-executive-order-12333-the-reagan-rule-that-lets-the-nsa-spy-on-americans/2014/07/18/93d2ac22-0b93-11e4-b8e5-d0de80767fc2_story.html.
48 Mark Jaycox, *Three Leaks, Three Weeks, and What We've Learned About the U.S. Government's Other Spying Authority: Executive Order 12333*, Electronic Frontier Foundation, November 5, 2013, https://www.eff.org/deeplinks/2013/10/three-leaks-three-weeks-and-what-weve-learned-about-governments-other-spying.
49 Barton Gellman and Ashkan Soltani, "NSA Collects Millions of E-mail Address Books Globally," *Washington Post*, October 14, 2013, https://www.washingtonpost.com/world/national-security/nsa-collects-millions-of-e-mail-address-books-globally/2013/10/14/8e58b5be-34f9-11e3-80c6-7e6dd8d22d8f_print.html.
50 Jaycox, "Three Leaks, Three Weeks, and What We've Learned About the U.S. Government's Other Spying Authority: Executive Order 12333."
51 Gellman and Soltani, "NSA Collects Millions of E-mail Address Books Globally," "This is not part of the PRISM collection under Section 702 of the Foreign Intelligence Surveillance Act (FISA) Amendments Act or the business records program under Section 215 of the PATRIOT Act, but a separate program called MUSCULAR under what appears to be Executive Order 12333."
52 Gellman and Soltani, "NSA Collects Millions of E-mail Address Books Globally."
53 Charlie Savage, "N.S.A. Gets More Latitude to Share Intercepted Communications," *New York Times,* January 12, 2017, https://www.nytimes.com/2017/01/12/us/politics/nsa-gets-more-latitude-to-share-intercepted-communications.html.
54 I use the full acronym PATRIOT throughout. I want to highlight the fact that the law has nothing to do with patriotism and its name has everything to do with marketing.
55 *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001*, P.L. 107-56)56), http://www.gpo.gov/fdsys/pkg/PLAW-107publ56/pdf/PLAW-107publ56.pdf.
56*Foreign Intelligence Surveillance Act of 1978* (FISA), http://www.gpo.gov/fdsys/pkg/STATUTE-92/pdf/STATUTE-92-Pg1783.pdf.
57*Electronic Communications Privacy Act of 1986* (ECPA), https://www.fpc.gov/electronic-communications-privacy-act-of-1986-ecpa/.
58 Attorney General John Ashcroft gave Congress one week in which to pass the bill—without changes—when the legislative proposals were introduced by the Bush administration in the aftermath of September 11. Vermont Democrat Patrick Leahy, chairman of the Senate Judiciary Committee, managed to convince the Justice Department to agree to some changes, and members of the House began to make significant improvements, many of which were removed in the final passage of the bill.
59 USA PATRIOT Act, Section 215, https://www.congress.gov/bill/107th-congress/house-bill/3162/text?q=%7B%22search%22%3A%5B%22USA+PATRIOT+Act%22%5D%7D&r=2.
60 This overview draws on Scott A. Boykin, "The Foreign Intelligence Surveillance Act and The Separation of Powers."
61 There is a Special Agent in Charge (SAIC) for each FBI Field Office, of which there are more than fifty - and this could be an Assistant SAIC (of which there are likely more), with no stipulation that the Field Office be relevant to the sought information.
62 Foreign Intelligence Surveillance Act of 1978 (FISA) 50 U.S. Code § 1804 – "Applications for Court Orders," https://www.law.cornell.edu/uscode/text/50/1804.
63 Foreign Intelligence Surveillance Act of 1978 (FISA) 50 U.S. Code § 1803 – "Designation of Judges." https://www.law.cornell.edu/uscode/text/50/1803.
64 Foreign Intelligence Surveillance Act 50 U.S.C. § 1804 (a)(b)(7). 42. 50 U.S.C. § 1801 (e); § 1805(a)(2)(A); § 1805(b).

65 American Bar Association, *Patriot Debates A Sourceblog for the USA PATRIOT Debate*, 2005, https://apps.americanbar.org/natsecurity/patriotdebates/act-section-215 (a) Subsection (2) An investigation conducted under this section shall-- "(A) be conducted under guidelines approved by the Attorney General under Executive Order 12333 (or a successor order); and "(B) not be conducted of a United States person solely upon the basis of activities protected by the first amendment to the Constitution of the United States.
66 This restriction was modified under reauthorization in 2005.
67 Civil Society Letters, Commentaries, and Testimony. "Section 702 Reauthorization Commentaries," "Warrantless Surveillance - Civil Society Letters," "Organizational Testimony-Warrantless Surveillance."
68 These are also known as "roving wiretaps."
69 U.S. Department of Justice, *Fact Sheet: USA PATRIOT Act Improvement and Reauthorization Act of 2005*, March 2, 2006, https://www.justice.gov/archive/opa/pr/2006/March/06_opa_113.html.
70 As a reminder, on June 5, 2013, Edward Snowden revealed that he had provided several reporters with access to documents he had taken from the National Security Agency.
71 Not case-by-case or one-by-one as the law allows, for records collectible under Section 215.
72 United States Foreign Intelligence Surveillance Court, Washington, DC, *In Re Application Of The Federal Bureau of Investigation For An Order Requiring The Production Of Tangible Things From Verizon Business Network Services,Inc. On Behalf Of MCI Communication Services, Inc. D/B/A Verizon Business Services*. Docket Number: BR 13-80.Signed April 25, 2013, https://www.theguardian.com/world/interactive/2013/jun/06/verizon-telephone-data-court-order.
73 Statement of Todd Hinnen, Acting Assistant Attorney General for National Security, Before the House Judiciary Subcommittee on Crime, Terrorism and Homeland Security, Washington DC, Wednesday, March 9, 2011, http://www.justice.gov/nsd/opa/pr/testimony/2011/nsd-testimony-110309.html.
74 Robert Chesney and Ben Wittes, "A Tale of Two NSA Leaks," *New Republic*, June 10, 2013, http://www.newrepublic.com/article/113427/nsa-spying-scandal-one-leak-more-damaging-other.
75 Michael Isikoff, "FBI Sharply Increases Use of Patriot Act Provision to Collect US Citizens' Records," *NBC News*, June 11, 2013, http://investigations.nbcnews.com/_news/2013/06/11/18887491-fbi-sharply-increases-use-of-patriot-act-provision-to-collect-us-citizens-records.
76 Statement of Todd Hinnen, March 9, 2011.
77 Intended to calm the waters post-Snowden. "This paper explains why the telephony metadata collection program, subject to the restrictions imposed by the Court, is consistent with the Constitution and the standards set forth by Congress in Section 215. Because aspects of this program remain classified, there are limits to what can be said publicly about the facts underlying its legal authorization. This paper is an effort to provide as much information as possible to the public concerning the legal authority for this program, consistent with the need to protect national security, including intelligence sources and methods.
78 This is an important point: We will learn that the NSA also used Section 215 to collect internet data in bulk.
79 See President's Surveillance Program below.
80 *Administration White Paper—Bulk Collection Of Telephony Metadata under Section 215 Of The USA PATRIOT Act*, August 9, 2013, https://fas.org/irp/nsa/bulk-215.pdf.
81 Horwitz and Branigin, "Lawmakers of both parties voice doubts about NSA surveillance programs."

82 Framed by Chair Robert Goodlatte as being about both how the collection of this metadata is relevant to a foreign intelligence or terrorism investigation (as required by Section 215) and how the government limits its targeting under 702 to non-U.S. persons outside the U.S...a description of the oversight performed by the administration and the FISC of this program, including the effectiveness of the current auditing of Section 702. See House of Representatives Committee on the Judiciary, "The Administration's Use of FISA Authorities," July 17, 2013, 3, https://judiciary.house.gov/wp-content/uploads/2016/02/113-45-81982.pdf.
83 As alluded to in the White Paper above.
84 Horwitz and Branigin, "Lawmakers of Both Parties Voice Doubts about NSA Surveillance Programs."
85 The NSA has since been limited to two hops.
86 Committee on the Judicary, *The Administration's Use of FISA Authorities*, House of Representatives, July 17, 113-1 (Washington, DC: Government Printing Office, 2013), 25, https://judiciary.house.gov/wp-content/uploads/2016/02/113-45-81982.pdf.
87 Horwitz and Branigin, "Lawmakers of Both Parties Voice Doubts about NSA Surveillance Programs.".
88 *Executive Order 12333*.
89 "Justice Department and NSA Memos Proposing Broader Powers for NSA to Collect Data," *Guardian*, June 7, 2013, https://www.theguardian.com/world/interactive/2013/jun/27/nsa-data-collection-justice-department.
90 *United States District Court for the Northern District of California Oakland Division, Case4:11-cv-05221-YGR Document63* Filed09/04/13, https://www.eff.org/files/filenode/20130904_doj_status_report.pdf.
91 Civil Society Letters, Commentaries, and Testimony. "Section 702 Reauthorization Commentaries," "Warrantless Surveillance - Civil Society Letters," "Organizational Testimony-Warrantless Surveillance."
92 *Electronic Frontier Foundation v. Department of Justice, NS-CA-0010, Docket 4:11-cv-05221-YGR (N.D. Cal),* October 26, 2011, https://www.clearinghouse.net/detail.php?id=13817.
93 *ACLU Files Lawsuit Challenging Constitutionality of NSA Phone Spying Program*, June 11, 2013, https://www.aclu.org/legal-document/aclu-v-clapper-complaint.
94 The May 7, 2015 ruling in United States Court of Appeals for the Second Circuit, below, is a ruling on *ACLU v. Clapper*.
95 "Verizon Forced to Hand Over Telephone Data - Full Court Ruling," *Guardian*, June 5, 2013, https://www.theguardian.com/world/interactive/2013/jun/06/verizon-telephone-data-court-order.
96 *United States District Court for the Northern District of California,* Filed09/04/13.
97 Not conducted, at least officially, under the auspices of Section 215, but contained in the release of documents.
98 *FISC Public Access Motions - ACLU Motion for Release of Court Records Interpreting Surveillance Under FISA*, https://www.aclu.org/legal-document/fisc-public-access-motions-aclu-motion-release-court-records-interpreting
99 *ACLU Motion for Release of Court Records Interpreting Surveillance Under FISA - FISC Public Access Motions*. November 6, 2013, https://www.aclu.org/legal-document/fisc-public-access-motions-aclu-motion-release-court-records-interpreting.
100 *United States Court of Appeals for the Second Circuit, Case 14-42 [ACLU v. Clapper], Document 168-1,* 05/07/2015,1503586, http://pdfserver.amlaw.com/nlj/NSA_ca2_20150507.pdf.
101 Known as Title III (of the Constitution) Courts.
102 *United States Court of Appeals for the Second Circuit, Case 14-42 [ACLU v. Clapper], Document 168-1,* 05/07/2015,1503586,

http://pdfserver.amlaw.com/nlj/NSA_ca2_20150507.pdf.
103 Ibid.
104 A separate argument, by the ACLU, that bulk collection of records about Americans is unconstitutional regardless of any laws that support it, was not addressed. *ACLU Files Lawsuit Challenging Constitutionality of NSA Phone Spying Program*, June 11, 2013.
105 *United States Court of Appeals for the Second Circuit, Case 14-42 [ACLU v. Clapper], Document 168-1,* 05/07/2015,1503586,
106 Charlie Savage and Jonathan Weisman, "N.S.A. Collection of Bulk Call Data Is Ruled Illegal," *New York Times*, May 7, 2015, https://www.nytimes.com/2015/05/08/us/nsa-phone-records-collection-ruled-illegal-by-appeals-court.html.
107 The latter was part of a 2004 intelligence law. *Intelligence Reform and Terrorism Prevention Act of 2004,"Lone Wolf" Amendment to the Foreign Intelligence Surveillance Act,"* https://www.gpo.gov/fdsys/pkg/PLAW-108publ458/pdf/PLAW-108publ458.pdf; Jim Abrams, "Patriot Act Extension Signed by Obama," HuffPost, May 27, 2011. http://www.huffingtonpost.com/2011/05/27/patriot-act-extension-signed-obama-autopen_n_867851.html.
108 Eric Lichtblau, "Senate Makes Permanent Nearly All Provisions of Patriot Act, With a Few Restrictions," *New York Times*, July 30, 2005, http://www.nytimes.com/2005/07/30/politics/senate-makes-permanent-nearly-all-provisions-of-patriot-act-with-a.html.
109 Clearly, E.O. 12333 predates it.
110 Boykin, "The Foreign Intelligence Surveillance Act and The Separation of Powers"
111 Offices of Inspectors General, *Unclassified Report on the President's Surveillance Program*, Report No. 2009-0013-AS, 2009.
112 James Risen and Eric Lichtblau, "Bush Lets U.S. Spy on Callers Without Courts," *New York Times*, December 16, 2005, http://www.nytimes.com/2005/12/16/politics/bush-lets-us-spy-on-callers-without-courts.html; James Risen and Eric Lichtblau, "Spy Agency Mined Vast Data Trove, Officials Report."
113 Risen and Lichtblau, "Bush Lets U.S. Spy on Callers Without Courts.".
114 The FISA Amendments Act of 2008 required the Inspectors General of Intelligence Community agencies that participated in the PSP (the Inspectors General (IGs) of the DoD, DOJ, CIA, NSA, and ODNI - collectively the "PSP IG Group") to conduct a comprehensive review of the program. The report is discussed below.
115 Rachel Levinson-Waldman, *What The Government Does With Americans' Data*, Brennan Center for Justice, 2013; footnote 348, https://www.brennancenter.org/publication/what-government-does-americans-data.
116 The cover term NSA used to protect the President's Surveillance Program. See Offices of Inspectors General of the Department of Defense, Department of Justice, Central Intelligence Agency, National Security Agency, Office of the Director of National Intelligence, *Fully Declassified Version Report on the President's Surveillance Program, Report No. 2009-0013-AS*, FN1, p.1.
117 Charlie Savage, "Government Releases Once-Secret Report on Post-9/11 Surveillance," *New York Times*, April 25, 2015, https://www.nytimes.com/interactive/2015/04/25/us/25stellarwind-ig-report.html.
118 Offices of Inspectors General, "*Unclassified Report on the President's Surveillance Program*, Report No. 2009-0013-AS, 2009..
119 Hayden was the NSA Director; Tenet was Secretary of Defense.
120 Signals Intelligence.
121 Offices of Inspectors General, "*Unclassified Report on the President's Surveillance Program*, Report No. 2009-0013-AS."
122 Risen and Lichtblau, "Bush Lets U.S. Spy on Callers Without Courts."

123 On which the *Times* sat for a year, at the request of the government and "to conduct additional reporting."
124 Since 2002.
125 Risen and Lichtblau, "Bush Lets U.S. Spy on Callers Without Courts."
126 Risen and Lichtblau, "Spy Agency Mined Vast Data Trove, Officials Report."
127 Electronic Frontier Foundation, *NSA Spying - How it Works,* https://www.eff.org/nsa-spying/how-it-works.
128 EFF's analysis is based on "the tremendous amount of information has been exposed by various whistleblowers, admitted to by government officials during Congressional hearings and with public statements, and reported on in investigations by major newspaper across the country. The government still considers the Program officially classified."
129 Offices of Inspectors General, *Unclassified Report on the President's Surveillance Program*, Report No. 2009-0013-AS, 2009.., footnotes 350,353.
130 The first version is the *Unclassified Report on the President's Surveillance Program*, Report No. 2009-0013-AS; the second *fully declassified* 747-page version was released on April 24, 2015, in response to a FOIA lawsuit brought by the *New York Times*: Offices of Inspectors General of the Department of Defense, Department of Justice, Central Intelligence Agency, National Security Agency, Office of the Director of National Intelligence *Fully Declassified Version Report on the President's Surveillance Program*, Report No. 2009-0013-AS, 2009.
131 Eric Lichtblau and James Risen, "U.S. Wiretapping of Limited Value, Officials Report," *New York Times*, July 10, 2009, http://www.nytimes.com/2009/07/11/us/11nsa.html.
132 For an in-depth overview of the efforts of Cheney and Bush to assert the unitary, indeed plenipotentiary power of the President, against especially Congress, watch http://www.pbs.org/wgbh/pages/frontline/cheney/.
133 Including the NSA's STELLARWIND program that mined information from email databases and gathered telephone metadata from the databases of cellphone service providers. The NSA also gathered and analyzed the content of telephone conversations and email communications from these databases.
134 See below under 2007 Memo.
135 Offices of Inspectors General of the Department of Defense, Department of Justice, Central Intelligence Agency, National Security Agency, Office of the Director of National Intelligence, *Unclassified Report on the President's Surveillance Program, Report No. 2009-0013-AS*.
136 Footnote 17 in *Unclassified Report on the President's Surveillance Program, Report No. 2009-0013-AS*.
137 Lichtblau and Risen, "U.S. Wiretapping of Limited Value."
138 Offices of Inspectors General, *Fully Declassified Version Report on the President's Surveillance Program, Report No. 2009-0013-AS*.; see also Office of the Director of National Intelligence, *The DOJ Releases Additional Information from IG Reports Concerning Collection Activities Authorized by President G.W. Bush After the Attacks of Sept. 11, 2001,* September 21, 2015, https://www.dni.gov/index.php/newsroom/press-releases/press-releases-2015/item/1254-the-doj-releases-additional-information-from-ig-reports-concerning-collection-activities-authorized-by-president-g-w-bush-after-the-attacks-of-sept-11-2001; and Charlie Savage, "Government Releases Once-Secret Report on Post-9/11 Surveillance," *New York Times*, April 25, 2015, https://www.nytimes.com/interactive/2015/04/25/us/25stellarwind-ig-report.html.
139 Charlie Savage, "Government Releases Once-Secret Report on Post-9/11 Surveillance."
140 Offices of Inspectors General, *Fully Declassified Version Report on the President's Surveillance Program, Report No. 2009-0013-AS*, FN 1, p. 1.
141 Barton Gellman, "U.S. Surveillance Architecture Includes Collection of Revealing Internet, Phone Metadata," *Washington Post,* June 15, 2013,

https://www.washingtonpost.com/investigations/us-surveillance-architecture-includes-collection-of-revealing-internet-phone-metadata/2013/06/15/e9bf004a-d511-11e2-b05f-3ea3f0e7bb5a_story.html
142 Offices of Inspectors General, *Fully Declassified Version Report on the President's Surveillance Program, Report No. 2009-0013-AS*. The fully declassified Report of the NSA IG begins on page 132 of the document.
143 Which points to those collections under E.O. 12333, discussed earlier.
144 Gellman, "U.S. Surveillance Architecture includes Collection of Revealing Internet, Phone Metadata."
145 Gellman, "U.S. Surveillance Architecture includes Collection of Revealing Internet, Phone Metadata."
146 Office of the Inspector General, National Security Agency Central Security Service, "ST-09-0002, Working Draft," March 24, 2009, https://www.documentcloud.org/documents/718895-igreport.html; initially published by Guardian and Washington Post, https://www.washingtonpost.com/apps/g/page/world/national-security-agency-inspector-general-draft-report/277/.
147 *United States District Court, Southern District of New York, "Complaint: The New York Times and Charlie Savage against National Security Agency,"NYT/Savage v. NSA, No. 15-2383 (Forrest, S.D.N.Y.) NYT/Savage complaint (March 31, 2015),* http://ia600502.us.archive.org/30/items/gov.uscourts.nysd.440331/gov.uscourts.nysd.440331.1.0.pdf.
148 Offices of Inspectors General, *Fully Declassified Version Report on the President's Surveillance Program, Report No. 2009-0013-AS*.
149 Discussed in detail below at Section 702/What We Learned.
150 Judge John D. Bates, *Memorandum Opinion*, United States Foreign Intelligence Court , October 3, 2011, http://www.scribd.com/doc/162016974/FISA-court-opinion-with-exemptions.
151 Office of the Director of National Intelligence, *The DOJ Releases Additional Information from IG reports. Concerning Collection Activities Authorized by President G.W. Bush After the Attacks of Sept. 11, 2001.*
152 Ellen Nakashima, "NSA Gathered Thousands of Americans' E-mails Before Court Ordered it to Revise its Tactics," *Washington Post*, August 21, 2013, https://www.washingtonpost.com/world/national-security/nsa-gathered-thousands-of-americans-e-mails-before-court-struck-down-program/2013/08/21/146ba4b6-0a90-11e3-b87c-476db8ac34cd_story.html.
153 As a result of an EFF FOIA lawsuit.
154 Ellen Nakashima, "Verizon Providing All Call Records to U.S. Under Court Order," *Washington Post,* June 6, 2013, https://www.washingtonpost.com/world/national-security/verizon-providing-all-call-records-to-us-under-court-order/2013/06/05/98656606-ce47-11e2-8845-d970ccb04497_story.html.
155 Judge John D. Bates, *Memorandum Opinion*.
156 Horwitz and Branigin, "Lawmakers of Both Parties Voice Doubts About NSA Surveillance Programs."
157 See Note 80.
158 "Justice Department and NSA Memos Proposing Broader Powers for NSA to Collect Data," *Guardian,* June 7, 2013, https://www.theguardian.com/world/interactive/2013/jun/27/nsa-data-collection-justice-department.
159 Horwitz and Branigin, "Lawmakers of Both Parties Voice Doubts About NSA Surveillance Programs."
160 The Upstream program discussed briefly above.

161 Horwitz and Branigin, "Lawmakers of Both Parties Voice Doubts About NSA Surveillance Programs.".
162 Discussed above in the section on E.O. 12333.
163 Eric Lichtblau and David Johnston, "Court to Oversee U.S. Wiretapping in Terror Cases," *New York Times*, January 18, 2007.
http://www.nytimes.com/2007/01/18/washington/18intel.html.
164 See David Kris' discussion of the breadth of such certifications below at Section 702.
165 U.S. Attorney General Alberto Gonzales surveillance memo, January 17, 2007; also *Leahy Response Congressional Record,* January 17, 2007, S646-S647,
http://news.findlaw.com/legalnews/us/terrorism/documents/index.html.
166 Judge Colleen Kollar-Kotelly, *Amendment to Order for Purposes of Querying the Metadata Archive [REDACTED], In re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things from [REDACTED], No. BR 07-10 (FISA Ct.* May 31, 2007) (authorizing collection of bulk telephone metadata under Section 215), United States Foreign Intelligence Surveillance Court, May 31, 2007,
https://www.aclu.org/files/section215/20140123/FISC%20Amended%20Order%20BR%2007-10.pdf.
167 Justice Department and NSA memos proposing broader powers for NSA, June 27, 2013.
168 Discussed previously.
169 Which here include the President's Surveillance Program/STELLARWIND and its successors.
170 The Intelligence Community uses this to indicate an excision of text.
171 The USA PATRIOT Act.
172 Judge Colleen Kollar-Kotelly, *Amendment to Order for Purposes of Querying the Metadata Archive [REDACTED], In re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things from [REDACTED], No. BR 07-10 (FISA Ct.* May 31, 2007) (authorizing collection of bulk telephone metadata under Section 215).
[173] Glenn Greenwald and Spencer Ackerman, NSA collected US email records in bulk for more than two years under Obama,· *Guardian*, June 27, 2013,
https://www.theguardian.com/world/interactive/2013/jun/27/nsa-data-collection-justice-department.
174 "NSA Collected U.S. Email records in Bulk for More than Two years Under Obama," *Guardian*, June 27, 2013; https://www.theguardian.com/world/2013/jun/27/nsa-data-mining-authorised-obama.
175 As far as discernable, reading between the substantial redactions.
176 Judge Colleen Kollar-Kotelly, *Opinion and Order,* United States Foreign Intelligence Court, date redacted, http://www.dni.gov/files/documents/1118/CLEANEDPRTT%201.pdf
177 Spencer Ackerman, "U.S. Admits Surveillance Violated Constitution At Least Once," *Wired*, July 20, 2012, https://www.wired.com/2012/07/surveillance-spirit-law/
178 Mark Rumold, *In Response to EFF Lawsuit, DOJ Releases 18 New Opinions of the FISC Concerning Section 702*, Electronic Frontier Foundation, June 14, 2017,
https://www.eff.org/deeplinks/2017/06/response-eff-lawsuit-doj-releases-18-new-opinions-fisc-concerning-section-702 .
179 Redacted, *CLEANED016. REDACTED BR06-05 Exhibits C (Memo of Law) and D-Sealed,* date redacted, in regard to Alberto R. Gonzales, and Other Redacted Persons, Application to United States Foreign Intelligence Court, May 23, 2006,
http://www.dni.gov/files/documents/1118/CLEANED016.%20REDACTED%20BR%2006-05%20Exhibits%20C%20%28Memo%20of%20Law%29%20and%20D-Sealed.pdf.
180 Redacted, *CLEANED016. REDACTED BR06-05 Exhibits C (Memo of Law) and D-Sealed,* date redacted, in regard to Alberto R. Gonzales, and Other Redacted Persons, Application to United States Foreign Intelligence Court, May 23, 2006, released to ACLU by Director of

National Intelligence, November 18, 2013, as result of a FOIA suit and containing additional unredacted signatories, https://www.aclu.org/foia-document/production-congress-may-23-2006-govt-memorandum-law.
181 Rachel Levinson-Waldman, "What The Government Does," 2013; Kate Martin, *Congressional Testimony 2006-2008,* Center for National Security Studies, http://cnss.org/pages/surveillance-cnss-work-on-surveillance-148.html; Julian Sanchez, "What the Ashcroft 'Hospital Showdown' on NSA Spying Was all About - How the Government Sought to Justify Blanket Collection of Internet Metadata," *Ars Technica,* July 29, 2013, https://arstechnica.com/tech-policy/2013/07/what-the-ashcroft-hospital-showdown-on-nsa-spying-was-all-about/.
182 50 U.S. Code § 1881a - "Procedures for Targeting Certain Persons Outside the United States Other Than United States Persons," https://www.law.cornell.edu/uscode/text/50/1881a.
183 Known colloquially, and quite confusingly, as the FAA.
184 Revealed in 2013 to be the PRISM program.
185 Julian Sanchez, *Confusion in the House: Misunderstanding Spying Law, and Inverting the Lessons of 9/11*, Cato Institute, September 13, 2012, https://www.cato.org/blog/confusion-house-misunderstanding-spying-law-inverting-lessons-911.
186 David S. Kris and J. Douglas Wilson, *National Security Investigations and Prosecutions* § 17:8 (2d ed., updated Aug. 2016), Westlaw NSIAP.
187 Julian Sanchez, *What the Manual by DOJ's Top Intelligence Lawyer Says about the FISA Amendments Act*, Cato Institute, August 21, 2012, quoting David Kris, above. https://www.cato.org/blog/what-manual-dojs-top-intelligence-lawyer-says-about-fisa-amendments-act.
188 Ali Watkins, "Most of NSA's Data Collection Authorized by Order Ronald Reagan Issued."
189 Declassified as a result of the Snowden disclosures.
190 Eric Lichtblau and James Risen, "Officials Say U.S. Wiretaps Exceeded Law," *New York Times*, April 15, 2009, http://www.nytimes.com/2009/04/16/us/16nsa.html.
191 Ibid.
192 Replicated in "NSA PRISM Program Slides," *Guardian*, November 1, 2013, https://www.theguardian.com/world/interactive/2013/nov/01/prism-slides-nsa-document and https://www.theguardian.com/world/2013/jun/08/nsa-prism-server-collection-facebook-google. See also note 33.
193 Risen and Lichtblau, "Spy Agency Mined Vast Data Trove, Officials Report."
194 To EFF as the result of a FOIA request.
195 Electronic Frontier Foundation, *FISC-Opinions-on-Sec-702-Released-06-14-2017*, Document Cloud, https://www.documentcloud.org/public/search/projectid:33596-FISC-Opinions-on-Sec-702-Released-06-14-2017; Chris Mirasola, Yishai Schwartz, *The 18 FISA Court Opinions on Section 702: Summaries*, Lawfare, June 23, 2017, https://www.lawfareblog.com/18-fisa-court-opinions-section-702-summaries.
196 United States Foreign Intelligence Court, *Memorandum Opinion,* October 2011, http://www.nytimes.com/interactive/2013/08/22/us/22nsa-opinion-document.html.
197 Upstream.
198 Judge John D. Bates, *Memorandum Opinion*.
199 Judge John D. Bates, *Memorandum Opinion*..
200 These activities were/are part of the National Security Agency's "upstream collection" (Upstream) which refers to the NSA getting a copy of Internet traffic as it flows through major telecommunications hubs, and searches through for "selectors," such as an email address (also known as "about" collection because the target is neither the sender or recipient of the communication, but instead was mentioned within the communication itself) or a keyword. In a press conference call on the newly declassified court opinion, the Office

of the Director of National Intelligence (ODNI) revealed new information about the way the NSA treated what it calls "multi-communication transactions." See Parker Higgins, *Intelligence Agency Attorney on How "Multi-Communication Transactions" Allowed for Domestic Surveillance*, Electronic Frontier Foundation, August 21, 2013, https://www.eff.org/deeplinks/2013/08/intelligence-agency-attorney-explains-how-multi-communication-transactions-allowed.
201 *Wyden Statement on Declassification of FISA Court Ruling on 4th Amendment Violations*, August 21, 2013, http://www.wyden.senate.gov/news/press-releases/wyden-statement-on-declassification-of-fisa-court-ruling-on-4th-amendment-violations.
202 Discussed in the next section of this article.
203 "Upstream" collection occurs as communications flow across Internet hubs. See Craig Timberg and Ellen Nakashima, "Agreements with Private Companies Protect U.S. Access to Cables' Data for Surveillance," *Washington Post*, July 6, 2013, https://www.washingtonpost.com/business/technology/agreements-with-private-companies-protect-us-access-to-cables-data-for-surveillance/2013/07/06/aa5d017a-df77-11e2-b2d4-ea6d8f477a01_story.html.
204 Nakashima, "NSA Gathered Thousands of Americans' E-mails."
205 Judge John D. Bates, *Memorandum Opinion*.
206 Higgins, "Intelligence Agency Attorney on How "Multi-Communication Transactions" Allowed for Domestic Surveillance."
207 Spencer Ackerman, "NSA Illegally Collected Thousands of Emails Before FISA Court Halted Program," *Guardian*, August 21, 2013, http://www.theguardian.com/world/2013/aug/21/nsa-illegally-collected-thousands-emails-court.
208 Ackerman, "NSA Illegally Collected Thousands of Emails Before FISA Court Halted Program.
209 Ackerman, "NSA Illegally Collected Thousands of Emails Before FISA Court Halted Program.
210 "Newly Disclosed N.S.A. Files Detail Partnerships With AT&T and Verizon," *New York Times*, August 15, 2015, https://www.nytimes.com/interactive/2015/08/15/us/documents.html.
211 *NYT ProPublica Fairview Stormbrew*, contributed by Charles Savage, *New York Times*, August 14, 2015, https://www.documentcloud.org/documents/2275521-nyt-propublica-fairview-stormbrew.html.
212 Kris and Wilson, *National Security Investigations and Prosecutions* § 17:8 (2d ed., updated Aug. 2016).
213 Eric Lichtblau, "In Secret, Court Vastly Broadens Powers of N.S.A.," *New York Times*, July 6, 2013, http://www.nytimes.com/2013/07/07/us/in-secret-court-vastly-broadens-powers-of-nsa.html.
214 The reauthorization of the FISA Amendments Act is discussed separately below.
215 Judge Rosemary M. Collyer, *FISC Memorandum and Opinion*, United States Foreign Intelligence Court, April 27, 2017, https://www.intelligence.gov/assets/documents/702%20Documents/declassified/2016_Cert_FISC_Memo_Opin_Order_Apr_2017.pdf.
216 Until April 2012.
217 Nakashima, "NSA Gathered Thousands of Americans' E-mails."
218 Judge Collyer, *FISC Memorandum and Opinion*.
219 National Security Agency/Central Security Service, "NSA Stops Certain Section 702 "Upstream" Activities," April 28, 2017, https://www.nsa.gov/news-features/press-room/statements/2017-04-28-702-statement.shtml.

220 Senator Ron Wyden, *Letter to Dan Coats, Director of National Intelligence*, July 31, 2017, https://www.wyden.senate.gov/download/letter-to-dni-coats-on-702-surveillance-august-3-2017.
221 Members of the House Judiciary Committee, *Letter to James Clapper, Director of National Intelligence*, April 22, 2016, https://fas.org/irp/congress/2016_cr/hjc-702.pdf.
222 Dustin Volz, "NSA Backtracks on Sharing Number of Americans Caught in Warrant-less Spying," *Reuters,* June 9, 2017, http://www.reuters.com/article/us-usa-intelligence-idUSKBN19031B.
223 Electronic Frontier Foundation, *Jewel v. NSA*, No. C 08-04373 (N.D. Cal. 2018), September 18, 2008, https://www.eff.org/files/filenode/jewel/jewel.complaint.pdf.
224 Ibid; see also Jamie Williams, "Jewel v. NSA Moves Forward - Time for NSA to Answer Basic Questions About Mass Surveillance," Electronic Frontier Foundation, June 21, 2016, https://www.eff.org/deeplinks/2016/06/jewel-v-nsa-moves-forward-time-nsa-answer-basic-questions-about-mass-surveillance.
225 Director, National Security Agency.
226 Electronic Frontier Foundation, "Federal Judge Allows EFF's NSA Mass Spying Case to Proceed," July 8, 2013, https://www.eff.org/press/releases/federal-judge-allows-effs-nsa-mass-spying-case-proceed.
227 Electronic Frontier Foundation, *Jewel v NSA*.
228 *Wikimedia Foundation v. NSA*, No. 15CV00662 (D. Md. 2015).
229 *See Order Granting Defendants' Motion to Dismiss*, *Wikimedia Foundation v. NSA*, No. 15CV00662, Dkt. 95 (filed Oct. 23, 2015); *Wikimedia Foundation v. NSA*, No. 15-2560 (4th Cir. 2016).
230 Reporters Committee for Freedom of the Press, The Thomas Jefferson Center for the Protection Of Free Expression, and 17 Media Organizations, as Amici Curiae in Support of Plaintiffs – Appellants, *Amicus Br. in Support of Plaintiffs-Appellants*, *Wikimedia v. NSA*, No. 15-2560 (4th Cir. filed Feb. 24, 2016), https://www.rcfp.org/sites/default/files/2016-02-24-wikimedia-v-nsa.pdf.
231 Rumold, "In Response to EFF Lawsuit, DOJ Releases 18 New Opinions of the FISC Concerning Section 702."
232 Rumold, "In Response to EFF Lawsuit, DOJ Releases 18 New Opinions of the FISC Concerning Section 702."
233 Rumold, "In Response to EFF Lawsuit, DOJ Releases 18 New Opinions of the FISC Concerning Section 702."
234 Civil Society Letters, Commentaries, and Testimony. "Section 702 Reauthorization Commentaries," "Warrantless Surveillance - Civil Society Letters," "Organizational Testimony-Warrantless Surveillance."
235 Drawn from Jodie Liu, "So What Does the USA Freedom Act Do Anyway?" *Lawfare*, June 3, 2015, https://www.lawfareblog.com/so-what-does-usa-freedom-act-do-anyway; for even more detail, see https://www.congress.gov/bill/114th-congress/house-bill/2048/summary/00.
236 The government maintains that its obligation to release such opinions does not apply to secret court rulings that predate the USA Freedom Act.
237 The Center for Constitutional Rights, "Surveillance After the USA Freedom Act: How Much Has Changed?" *Huffington Post*, December 17, 2016, http://www.huffingtonpost.com/the-center-for-constitutional-rights/surveillance-after-the-us_b_8827952.html; see also Caroline Lynch and Lara Flint, "The USA FREEDOM Act Turns Two," *Lawfare*, June 2, 2017, https://www.lawfareblog.com/usa-freedom-act-turns-two.
238 Civil Society Letters, Commentaries, and Testimony. "Section 702 Reauthorization Commentaries," "Warrantless Surveillance - Civil Society Letters," "Organizational Testimony-Warrantless Surveillance."

239 American Civil Liberties Union, *Motion of the American Civil Liberties Union for the Release of Court Records*, United States Foreign Intelligence Court, October 18, 2016, https://www.aclu.org/legal-document/aclu-motion-filed-foreign-intelligence-surveillance-court-fisc-requesting-release.
240 115th Congress**,** 1st Session, *H.R. 2144, Uniting and Strengthening America by Reforming and Improving the Government's High-Tech Surveillance Act*, October 25, 2017, https://www.congress.gov/bill/115th-congress/house-bill/4124.
241 Brennan Center for Justice, "FISA Reauthorization Amendments Act (S.139) compared with Amash/USA RIGHTS Acts Amendment," January 10, 2018.
242 115th Congress**,** 2nd Session, *S. 139, FISA Amendments Reauthorization Act of 2017*, January 11, 2018, https://www.congress.gov/bill/115th-congress/senate-bill/139/text.
243 Michelle Richardson, "FISA 702: What Happened and What's Next," Center for Democracy and Technology, February 5, 2018, https://cdt.org/blog/fisa-702-what-happened-and-whats-next/.
244 National Security Agency/Central Security Service, "NSA Stops Certain Section 702 "Upstream" Activities."
245 Loretta Lynch, Attorney General of the United States, *Minimization Procedures Used by the Federal Bureau of Investigation in Connection with Acquisition of Foreign Intelligence Information Pursuant to Section 702 of the Foreign Intelligence Surveillance Act, as Amended*, September 21, 2016, https://www.dni.gov/files/documents/icotr/51117/2016_FBI_Section_702_Minimization_Procedures_Sep_26_2016_part_1_and_part_2_merged.pdf.
246 Brennan Center for Justice, "FISA Reauthorization Amendments Act (S.139) compared with Amash/USA RIGHTS Acts Amendment."
247 But note Title III of USA FREEDOM, which prohibits the use, in court proceedings, of information obtained under Section 702 through procedures deemed by a FISA Court to be "deficient concerning any United States person." Nor may the government "use[] or disclose[] in any other manner" such information.
248 The Brennan table notes "Current law requires the government to provide notification to people when 702-derived information is used against them in legal proceedings, but the government has reportedly interpreted this requirement extremely narrowly and is not giving notification in many cases. Moreover, when Americans have tried to challenge Section 702 surveillance, courts have held that they aren't "injured" by Section 702 surveillance, and therefore can't challenge it, unless they can prove that their communications have been incidentally collected - which is an impossible Catch 22, given the secrecy of the surveillance."
249 According to the Center for Democracy and Technology. See Michelle Richardson, "FISA 702: What Happened and What's Next."
250 Savage, "Fight Brews Over Push to Shield Americans," May 6, 2017.
251 The White House, "Presidential Policy Directive/PPD-19," Washington, DC, October 10, 2012, https://www.va.gov/ABOUT_VA/docs/President-Policy-Directive-PPD-19.pdf.
252 Civil Society Letters, Commentaries, and Testimony. "Section 702 Reauthorization Commentaries," "Warrantless Surveillance - Civil Society Letters," "Organizational Testimony-Warrantless Surveillance."
253 *Administration White Paper - Bulk Collection Of Telephony Metadata under Section 215 Of The USA PATRIOT Act*, August 9, 2013, https://fas.org/irp/nsa/bulk-215.pdf.
254 Benjamin Wittes, Raffaela Wakeman, and Ritika Singh, "The NSA Documents, Part V: The Communications with Congress," *Lawfare*, August 22, 2013, http://www.lawfareblog.com/2013/08/the-nsa-documents-part-v-the-communications-with-congress/; Ellen Nakashima, "Lawmakers Increase Calls for NSA reform," *Washington Post*, August 16, 2013, https://www.washingtonpost.com/world/national-security/lawmakers-privacy-advocates-call-for-reforms-at-nsa/2013/08/16/7cccb772-0692-11e3-a07f-

49ddc7417125_story.html; Ritika Singh, "Congress on the FISA Order and Data Mining Stories," *Lawfare,* June 7, 2013, https://www.lawfareblog.com/congress-fisa-order-and-data-mining-stories; Janet Hook, "Lawmakers' Mixed Reactions on NSA Surveillance of Phone Records," Washington Wire, *Wall Street Journal*, June 6, 2013, https://blogs.wsj.com/washwire/2013/06/06/congress-reacts-to-nsa-surveillance-of-phone-records/.
255 Ritika Singh, "Congress on the FISA Order and Data Mining Stories."
256 Risen and Lichtblau, "Bush Lets U.S. Spy on Callers Without Courts."
257 Noted above under the section on the President's Surveillance Program.
258 Senator Jay Rockefeller, Vice-Chairman, Senate Select Committee on Intelligence, hand-written to Vice President Cheney, July 17, 2003, https://fas.org/irp/news/2005/12/rock121905.pdf.
259 Charles Babington and Dafna Linzer, "Senator Sounded the Alarm in '03," *Washington Post*, December 20, 2005, http://www.washingtonpost.com/wp-dyn/content/article/2005/12/19/AR2005121901641.html.
260 Spencer Ackerman, "Intelligence Committee Withheld Key File Before Critical NSA Vote, Amash Claims," *Guardian*, August 12, 2013, http://www.theguardian.com/world/2013/aug/12/intelligence-committee-nsa-vote-justin-amash.
261 Peter Wallsten, "House Panel Withheld Document on NSA Surveillance Program from Members," *Washington Post*, August 16, 2013, http://www.washingtonpost.com/politics/house-panel-withheld-document-on-nsa-surveillance-program-from-members/2013/08/16/944e728e-0672-11e3-9259-e2aafe5a5f84_story.html.
262 Now Ranking Member.
263 Watkins, "Most of NSA's Data Collection Authorized by Order Ronald Reagan Issued."
264 Ibid.
265 Ibid.
266 Eight Members, House Intelligence Committee, "Letter to the Chair and Ranking Member of the House Appropriations Committee," March 22, 2016, https://fas.org/irp/congress/2016_cr/hpsci-hac.pdf.
259 Eight Members, House Intelligence Committee, "Letter to the Chair and Ranking Member of the House Appropriations Committee," March 22, 2016.
260 Thirty-three Civil Society Organizations, Letter to Speaker Ryan and Minority Leader Pelosi, "Strengthening Congressional Oversight of the Intelligence Community," September 13, 2016, https://s3.amazonaws.com/demandprogress/letters/Strengthening_Congressional_Oversight_of_the_IC_Letter_Sept_2016.pdf.

269 Select Committee To Study Governmental Operations, Intelligence Activities And The Rights Of Americans, *Book III, Supplementary Detailed Staff Reports on Intelligence Activities and the Rights of Americans*, S. Rep. No. 94-755, at 10–13 (1976), https://www.intelligence.senate.gov/sites/default/files/94755_III.pdf
270 Civil Society Organizations, "Strengthening Congressional Oversight of the Intelligence Community."
271 Heidi Kitrosser, "Congressional Oversight of National Security Activities: Improving Information Funnels," 29 *Cardozo L. Rev.* 1049 (2008), https://scholarship.law.umn.edu/faculty_articles/86.
272 Kathleen Clark, "Congress's Right to Counsel in Intelligence Oversight." *University of Illinois Law Review* 2011 (June 2011), 915-960, Washington University in St. Louis Legal Studies Research Paper No. 11-01-01, https://ssrn.com/abstract=1744422.
273 Foreign Intelligence Surveillance Act, P.L. 95–511, 92 Stat. 1783, 50 U.S.C. ch. 36.

274 USA FREEDOM provides for the appointment of amici curiae to assist the FISA Court, who may provide assistance with respect to "legal arguments or information regarding any ... area relevant to the issue presented to the court," *but only if the FISA Court deems such information relevant and only in certain matters that "present ... a novel or significant interpretation of the law" in the eyes of the FISA Court.* [emphasis added]
275 Lichtblau, "In Secret, Court Vastly Broadens Powers of N.S.A."
276 In the 2012 FISA Amendments Act reauthorization, Section 702.
277 In the 2012 FISA Amendments Act reauthorization.
278 United States District Court for the Northern District of California Oakland Division, *Case4:11-cv-05221-YGR Document63* Filed09/04/13, https://www.eff.org/files/filenode/20130904_doj_status_report.pdf.
279 *Case 4:11-cv-05221-YGR Document1* Filed10/26/11.
280 CBS DC, "DOJ Declassifying Portions Of Secret Foreign Intelligence Surveillance Court Opinions," September 5, 2013, http://washington.cbslocal.com/2013/09/05/doj-declassifying-portions-of-secret-foreign-intelligence-surveillance-court-opinions/.
281 Electronic Frontier Foundation, *Title I ("Classic") FISA opinions*, https://www.documentcloud.org/public/search/projectid:37198-FISC-Opinions-on-classic-FISA-Released-01-31-2018; *Business Records & PR/TT provisions of FISA*, https://www.documentcloud.org/public/search/projectid:35411-FISC-Opinions-on-PR-TT-Released-09-25-2017; *Section 702 opinions*, https://www.documentcloud.org/public/search/projectid:33596-FISC-Opinions-on-Sec-702-Released-06-14-2017.
282 Emily Berman, "The Two Faces of the Foreign Intelligence Surveillance Court," *Indiana Law Journal* 91, no.4 (2016), http://www.repository.law.indiana.edu/ilj/vol91/iss4/4.
283 Robert Stein, Walter Mondale, and Caitlinrose Fisher, "No Longer a Neutral Magistrate: The Foreign Intelligence Surveillance Court in the Wake of the War on Terror," 100 *Minn. L. Rev*. 2251 (2016), http://scholarship.law.umn.edu/faculty_articles/564.
284 Mondale, while a Senator, served as a member of the Church Committee and as chairman of the subcommittee that drafted the Church Committee's final report on domestic intelligence activities, and, as Vice President, was instrumental to the enactment of FISA.
285 The FISC has provided an index of *Public Filings U.S. Foreign Intelligence Surveillance Court Beginning June 2013,* http://www.fisc.uscourts.gov/public-filings; the ODNI information on declassified FISC opinions - interspersed with other information related to the FISC - is to be found on icontherecord/tumblr.com. *IC ON THE RECORD POSTS TAGGED:"fisc."* See https://icontherecord.tumblr.com/tagged/fisc.
286 On which you may find what you are looking for, or may not be able to. IC on the Record, https://icontherecord.tumblr.com/. The name is variously pronounced, depending on the perspective of the person saying it: "Since its launch in August 2013, IC on the Record has provided a central hub for Intelligence Community–related official statements, declassified documents, congressional testimony, transparency reporting and multimedia content, making these materials more readily available and broadly accessible than ever before." See also https://www.dni.gov/index.php.
287 Josh Gerstein, "Intelligence Agencies Tout Transparency," *Politico,* February 3, 2015, http://www.politico.com/blogs/under-the-radar/2015/02/intelligence-agencies-tout-transparency-202023.
288 ODNI Office of Civil Liberties, Privacy and Transparency, *Updated Guide to Posted Documents Regarding Use of National Security Authorities – as of December 4, 2017,* https://www.dni.gov/files/documents/icotr/Updated-Guide_to_Posted_Documents_December_2017_FINAL.pdf.
289 Intel.gov. https://www.intel.gov.

290 The INTEL Vault, https://www.intel.gov/intel-vault.
291 Email communication.
292 Kevin Poulsen, "U.S. Intelligence Shuts Down Damning Report on Whistleblower Retaliation," *Daily Beast*, February 11, 2018, https://www.thedailybeast.com/us-intelligence-shut-downs-damning-report-on-whistleblower-retaliation.
293 United States District Court, Northern District of California, Oakland Division, *In Camera, Ex Parte Declaration of Elizabeth B[], Deputy Director of Capabilities, National Security Agency, Carolyn Jewell, et al, Plaintiffs, National Security Agency, et al., Defendants*, October 5, 2017, https://www.politico.com/f/?id=00000161-10d3-d990-af71-f8f7a0010001.
294 Josh Gerstein, "NSA Deleted Surveillance Data it Pledged to Preserve," *Politico*, January 19, 2018. https://www.politico.com/story/2018/01/19/nsa-deletes-surveillance-data-351730; see also Office of the Director of National Intelligence, *NSA Reports Data Deletion*, June 28, 2018, http://icontherecord.tumblr.com/.
295 DNI James Clapper, "Introduction to the 3rd Annual Sigint Progress Report," January 18, 2017, https://icontherecord.tumblr.com/ppd-28/2017/introduction.
296 In addition to the quotes from Litt and Clapper, see Army Lt. Gen. Michael T. Flynn, Director of the Defense Intelligence Agency: "Transparency has to be a watchword for the intelligence community if it is to regain the public's trust," in Claudette Roulo, "DIA Chief: Transparency Builds Public Trust," *DoD News*, July 27, 2014, https://www.defense.gov/News/Article/Article/602955/dia-chief-transparency-builds-public-trust/; see also then-CIA Director John Brennan: "CIA and the rest of the intelligence community have to maintain the requisite level of public confidence in order to do our jobs effectively," https://gwtoday.gwu.edu/security-chiefs-discuss-national-security-and-public-trust-cia-forum; and Michael Hayden, "If we are going to conduct espionage in the future, we are going to have to make some changes in the relationship between the intelligence community and the public it serves," quoted in George Packer, "Can You Keep a Secret? The former C.I.A. Chief Michael Hayden on Torture and Transparency," *New Yorker,* March 7, 2016, https://www.newyorker.com/magazine/2016/03/07/michael-hayden-comes-out-of-the-shadows.
297 Patrice McDermott, "Exec Dir McDermott Delivers Remarks on Improving the Security Classification System," *OpenTheGovernment.org*, December 8, 2016, http://www.openthegovernment.org/node/5379.
298James Madison, letter to W.T. Barry, August 4, 1822.
299 *Executive Order 13526: Classified National Security Information*, Sec. 1.7. *Classification Prohibitions and Limitations.* (a) In no case shall information be classified, continue to be maintained as classified, or fail to be declassified in order to: (1) conceal violations of law, inefficiency, or administrative error; (2) prevent embarrassment to a person, organization, or agency; see https://www.archives.gov/isoo/policy-documents/cnsi-eo.html#one.
300 For an analysis of how coverage has waxed and waned. See Elizabeth Hempowicz, "Busting the Myth of Whistleblower Protections for IC Contractors," *Project on Government Oversight,* September 20, 2016, http://www.pogo.org/blog/2016/09/protect-whistleblowers-ic-contractors.html.
301 United States Senate Select Committee on Intelligence, *Intelligence Authorization Act For Fiscal Year 2018, Report together with Additional And Minority Views [To accompany S. 1761],* September 7, 2017, https://fas.org/irp/congress/2017_rpt/ssci-fy2018.html.
302 Intelligence Community employees have protection under President Obama's 2012 *Presidential Policy Directive 19*, Part A, https://www.va.gov/ABOUT_VA/docs/President-Policy-Directive-PPD-19.pdf.
303 Jenna McLaughlin, "A Turf War Is Tearing Apart the Intel Community's Watchdog Office: Internal Scuffling Threatens to Dismantle the Intelligence Community Inspector

General," *Foreign Policy*, October 18, 2017, http://foreignpolicy.com/2017/10/18/turf-war-intelligence-community-watchdog-falling-apart/; Charles S. Clark, "Is the Intel Community's Whistleblower Outreach Being Shut Down?," *Government Executive*, October 20, 2017, http://www.govexec.com/management/2017/10/intel-communitys-whistleblower-outreach-being-shut-down/141946/; Charles Clark, "Embattled Intelligence Whistleblower Ombudsman Defends Himself," *Government Executive*, January 17, 2018, http://www.govexec.com/oversight/2018/01/embattled-intelligence-whistleblower-ombudsman-defends-himself/145249/.

304 These include Government Accountability Project (GAP) – on whose board I serve – and the Project on Government Oversight (POGO).

305 Civil Society Letters, Commentaries, and Testimony. "Section 702 Reauthorization Commentaries," "Warrantless Surveillance - Civil Society Letters," "Organizational Testimony-Warrantless Surveillance."

306 Just Security, https://www.justsecurity.org.

307 Lawfare - Hard National Security Choices, https://www.lawfareblog.com/.

308 Gerstein, "NSA Deleted Surveillance Data it Pledged to Preserve."