THE CENTURY FOUNDATION

REPORT SURVEILLANCE & PRIVACY

Reining In Warrantless Wiretapping of Americans

MARCH 16, 2017 — JENNIFER GRANICK

The United States is collecting vast amounts of data about regular people around the world for foreign intelligence purposes. Government agency computers are vacuuming up sensitive, detailed, and intimate personal information, tracking web browsing,[1] copying address books,[2] and scanning emails of hundreds of millions of people.[3] When done overseas, and conducted in the name of foreign intelligence gathering, the collection can be massive, opportunistic, and targeted without any factual basis. While international human rights law recognizes the political and privacy rights of all human beings, under U.S. law, foreigners in other countries do not enjoy free expression or privacy rights, so there are few rules and little oversight for how our government uses foreigners' information. And while foreign governments are certainly legitimate targets for intelligence gathering, reported spying on international social welfare organizations like UNICEF and Doctors Without Borders raises the specter of political abuse without a clear, corresponding national security benefit.[4]

In my book, *American Spies: Modern Surveillance, Why You Should Care, and What To Do About It*,[5] I explain the dangers that massive collection of information about Americans poses to our democracy. Soon, there will be an opportunity to rein in some of this surveillance. In December 2017, one of the laws enabling the National Security Agency (NSA) to warrantlessly wiretap Americans' international communications and to gather foreigners' private messages from top Internet companies will expire. The expiration forces Congress to decide whether to renew the law, reform it, or kill it. Because the surveillance law allows spying so far afield of national security interest, critics argue that it should be markedly curtailed, or allowed to end.

This report first reviews the most problematic aspects of this surveillance law. It then takes a deeper dive into the birth, justification, use—and abuse—of this law, and underscores key issues areas that call out the most for its reform.

The Notorious Section 702

The law in question—section 702 of the Foreign Intelligence Surveillance Act (FISA) Amendments Act—is notorious as the legal basis for two of the U.S. government's most controversial surveillance programs operating *inside the United States*. In June of 2013, former National Security Agency (NSA) contractor Edward Snowden helped reveal to the world these two NSA programs—called PRISM and Upstream—that take place under section 702.

Section 702, passed in 2008 as part of the FISA Amendments Act, authorized intelligence agencies to warrantlessly spy on foreigners located overseas. In the process of doing this through PRISM and Upstream, however, the NSA cannot help but collect large volumes of Americans' communications as well. Some of this collection takes place when Americans at home are talking with NSA targets abroad. But Americans' communications are also collected when they

are talking with friends abroad about targets, or when the NSA's machines inadvertently suck in Internet transactions that contain messages irrelevant to the target. The U.S. government calls this collection "incidental," but it includes vast amounts of Americans' conversations, email exchanges, photos, and other sensitive information. Moreover, once this information is collected, Americans' messages may be kept and searched by multiple government agencies, without a search warrant, without a factual predicate, and for a variety of purposes having nothing to do with foreign intelligence or national security.

The documents describing Upstream surveillance in particular provided new details to longstanding allegations that intelligence agencies as common practice search the stream of messages flowing over the telecommunications backbone for particular selectors, or search terms. Under the Upstream program, the documents show, the NSA's warrantless wiretapping directly on the Internet backbone inside the United States captures irrelevant messages, Americans' international messages, and even purely domestic exchanges.

Independent analysis of one large sample of data collected under section 702 suggest that non-targeted communicants end up in the section 702 trawl at ten times the rate of those of actual targets.[6] These revelations caused an outcry among Americans, Europeans, and people around the world.

While section 702 is credited with a number of (classified) national security successes,[7] its footprint is far broader than that. Section 702 programs gather vast amounts of information about a broad range of foreigners, including when they talk to Americans and what they say. This collection is not limited to national security interests, but to any matter of foreign intelligence. Foreign intelligence is defined quite broadly; surveillance can take place under 702 merely to gather information in order to better conduct foreign affairs.

Once intelligence agents collect private messages under section 702, domestic law enforcement agencies are authorized to use the sensitive data in a range of worrisome ways. The Federal Bureau of Investigation (FBI) may search the information to learn whether Americans are committing run-of-the-mill crimes without any pre-existing suspicion. Normally, conversations people have with their attorneys are treated as privileged information: no one can compel a lawyer to testify against his or her client. However, the NSA does not recognize that privilege.[8] Only when a lawyer is representing a client in an ongoing criminal case are attorney-client communications given special treatment. Otherwise, the NSA treats client consultations on how to avoid or respond to potential criminal exposure, as well as all consultations and representations about civil matters, the same as any other conversation. Encrypted materials may be kept indefinitely.[9] There are even fewer restrictions on what can be done with foreigners' data. Further, these databases

are magnets for insider abuse—there are documented cases of agents using databases of private information to spy on their lovers or spouses,[10] though we do not know how common this is, or how effective the agencies are at ferreting out wrongdoing.

Excessive surveillance can be an impediment, resulting in a confusing information glut that means intelligence officials miss important clues.

The public seems to intuitively believe that surveillance makes us safer. In some cases that is true, but it is not uniformly the case. Not all information is useful in ferreting out dangers. Indeed, excessive surveillance can be an impediment, resulting in a confusing information glut that means intelligence officials miss important clues. For example, classified slides describing one overseas bulk collection program reveal that numerous intelligence analysts have complained about the program and the relatively small intelligence value it provides as compared to the sheer volume of collection.[11] This "analysis paralysis" is a serious problem at the NSA.[12] A number of internal documents entitled "Data Is Not Intelligence," "The Fallacies Behind the Scenes," "Cognitive Overflow?" "Summit Fever," and "In Praise of Not Knowing" discuss the problem of having so much information, you don't know what to do with it.

Human nature and history show that loosely regulated spying is itself dangerous. After World War II, the U.S. Census Bureau sent block-by-block data on the locations of Japanese Americans to the War Department so that these families could be rounded up and imprisoned in internment camps.[13] For years, the FBI deliberately sought intelligence embarrassing to senators to gain political advantage. Agents concocted false charges[14] and threatened senators with revealing embarrassing information to gain compliance in political battles.[15] The U.S. government spied on, and even threatened, Dr. Martin Luther King Jr. and his allies in an effort to dissuade them from their activism.[16] In 1964, the FBI used information obtained from surveillance to plant false documents to create rifts in the American Communist Party.[17] In the 1980s, the U.S. government listened to service members' phone calls and read their mail in order to identify and dishonorably discharge homosexuals in the armed services.[18] The New York City Police Department has conducted secret monitoring of American Muslims, scaring people away from practicing their faith and from providing social services or making charitable contributions through their mosques.[19]

This issue, then, is not about privacy versus security. It is about balancing personal and political security with national security.

On December 31, 2017, section 702 will expire, unless Congress reauthorizes it. This "sunset" is a great opportunity to

revisit section 702 in light of these problems, and to reform it. If Congress finds that section 702 is worth keeping in some form, then there are three critical issue areas where Congress should consider reforming the law.

First, Congress should consider the scope of collection under section 702. Is the current broad scope of collection the proper use of intelligence resources, given the international uproar over privacy harms, or should Congress reduce the scope of collection so that it focuses on national security? Second, should Congress ensure that the subsequent retention and use of section 702 data does not repurpose information opportunistically collected for legitimate national security purposes for criminal assessments that give the Federal Bureau of Investigation a window into Americans' private lives and political activities? Third, should Congress shore up the mechanisms for accountability to ensure that the safeguards imposed on government surveillance powers are followed, and to assure everyone—including Americans at home and foreign customers of U.S. businesses—that new technologies are not being abused in disservice to civil liberties?

Why Do We Even Have Section 702?

After the terrorist attacks on September 11, 2001 brought down the World Trade Center towers, President George W. Bush's administration scrambled to augment the government's capacity to identify future unknown terrorist threats. In service of this goal, the Bush administration started a series of massive information-gathering projects, collectively known by the top secret cover name STELLARWIND. STELLARWIND involved new, warrantless collection of four kinds of data: telephone content (words spoken), telephone metadata (numbers dialed), Internet content (words in emails and other online messaging), and Internet metadata (non-content information from digital messages and transactions). STELLARWIND was a top secret program, because the various types of collection likely violated either statutory law, the Fourth Amendment of the U.S. Constitution, or both.

In 2004, the Bush administration ran into trouble with STELLARWIND. Acting Attorney General James Comey refused to sign off on part of the program, forcing the White House to go to the secretive Foreign Intelligence Surveillance Court (FISC) for approval. Then in December 2005, thanks to a whistleblower from the Office of Intelligence Policy and Review (OIPR), the part of the United States Department of Justice (DOJ) responsible for green-lighting American surveillance within the executive branch, the public learned about the warrantless wiretapping aspect of STELLARWIND in a *New York Times* article.[20] The disclosure of the illegal wiretapping, in combination with the internal disagreements over whether other aspects of STELLARWIND were properly authorized, forced the intelligence community to try to legitimize at least some aspects of the warrantless wiretapping program in the FISC and in Congress. Ultimately, American spies successfully obtained legislative approval for STELLARWIND-style warrantless wiretapping when Congress passed the FISA Amendments Act of 2008.

Section 702 is part of that act. Section 702 allows the government to warrantlessly collect, with the compelled cooperation of electronic service providers, the contents of electronic communications, including telephone calls and emails, where the target is reasonably believed to be a non-U.S. person located outside the United States.[21] Criminal authorities may use these warrantless procedures, so long as the foreign intelligence-gathering goal is a "significant purpose" of the collection.[22]

Under section 702, intelligence agencies obtain broad topical certifications from the FISC to investigate categories of foreign intelligence.[23] Once a certification issues, intelligence officers create lists of targets on which they will collect information related to the certification topic. The targets must be non-U.S. persons believed to be located abroad. "Directives" containing selectors, or search terms, designed to gather information about that target are then sent to service providers such as Google, Yahoo!, Apple, and Microsoft. The directives compel those companies to use the listed selectors to search their available data and identify responsive information, including both metadata and the contents of communications. While the certifications are reviewed and approved by a judge appointed to the FISC, and the targeting procedures are also approved, the targeting decisions, the directives, and the selectors, are exclusively within the Executive Branch's discretion.[24] In other words, neither Congress nor the intelligence court knows the identities of the targets or the basis for their selection.

To be sure, foreign intelligence collection serves important national security goals. Terrorism, weapons proliferation, network attacks on government infrastructure, and counterintelligence are critical priorities. Today, these are diffuse and complex threats. There are newly powerful political actors on the international stage. Organizations that are not governments and have no physical territory can inflict great harm. And individuals and diffuse coalitions are increasingly able to traffic in military technology, advanced computer malware, and other dangerous, potentially lethal tools. These challenges are real, and overcoming them are legitimate goals of surveillance.

But section 702 goes beyond permitting intelligence-gathering on national security topics. The targets of the surveillance need only be non-U.S. persons, reasonably believed to be located abroad, and connected in some way to one of the broad certification topics approved by the FISC. Intelligence analysts need not have any cause to believe that the target is involved in illegal activity, nor working for a terrorist group or foreign government. Surveillance can occur for any foreign intelligence purpose related to "the conduct of the foreign affairs of the United States."[25]

Where Section 702 Goes Astray

A recently declassified FISC opinion from November 2015 confirmed what many people already suspected—section 702 actually sweeps up "substantial quantities" of information concerning U.S. persons.[26] In other words, the surveillance program subjects Americans to extensive, warrantless surveillance. This broad collection of communications may be politically palatable when Americans are talking to terrorists—the implication is that this "incidental" collection is minor and necessary for public safety. However, foreign targets are not necessarily terrorism suspects, or wrongdoers of any kind. Section 702 contemplates surveillance targeting bureaucrats, scientists, aid workers—anyone of "foreign intelligence" interest.[27] Because the sanctioned surveillance topics are so broad, a vast number of people, including Americans, routinely have their communications swept up with no national security benefit attached.

The way politicians talk about section 702 masks the true purpose of the statute. When Americans talk to targets, or talk with friends overseas *about* targets,[28] the government warrantlessly gathers those phone calls, emails, and chats. Before the law was passed, Americans' international communications were off limits—protected by both FISA and the Electronic Communication Privacy Act (ECPA) from warrantless acquisition. Section 702 changed that, approving warrantless surveillance of Americans talking to some foreigners, even if it wasn't immediately obvious to non-experts that that was the case.

Government officials have consistently insisted that section 702 does not impact Americans[29] and to date, officials have repeatedly refused to estimate the number of Americans whose conversations have been collected.[30] The public doesn't know how big of an impact section 702 has on American privacy. However, there are reasons to be very concerned. *The Washington Post* studied a sample data set of information it obtained from Edward Snowden. The data had been collected under section 702 and reviewed and minimized by NSA analysts. The information included very personal material: "medical records sent from one family member to another, résumés from job hunters, and academic transcripts of schoolchildren. In one photo, a young girl in religious dress beams at a camera outside a mosque."[31] The data included "scores" of pictures of infants and toddlers in bathtubs, on swings, sprawled on their backs, and being kissed by their mothers. There was also more intimate, risqué content: men showing off their bodies, women wearing lingerie or swimsuits posing suggestively for the camera.

Many of the people in the data trove are Americans. More than half of the surveillance files contained names, email addresses, or other details that the NSA marked as belonging to U.S. citizens or residents.[32]

Insider abuse is another huge problem. A network of rules, regulations, and procedures tries but sometimes fails to stop government employees from using sensitive personal information to spy on their spouses or lovers. This problem is common enough that agencies call it LOVEINT, a parody name modeled on signals intelligence (SIGINT) and human intelligence (HUMINT). Harold Thomas Martin, a former NSA contractor, has been accused of stealing highly sensitive

government material related to national defense from the U.S. intelligence community.[33] NSA officials initially denied that Edward Snowden's position as an NSA contractor would have given him access to private data collected under section 702, but he nevertheless had such access.[34]

Ultimately, the reason people worry about broad surveillance is the danger that private information will be abused for political reasons.

Ultimately, the reason people worry about broad surveillance is the danger that private information will be abused for political reasons. U.S. history is replete with examples of government surveillance being used against disfavored groups based on race, political values, and sexual orientation. Most Americans know that during the J. Edgar Hoover era, peaceful people like Dr. Martin Luther King and Muhammad Ali were under surveillance for First Amendment–protected activities, or for no clear reason at all. A common narrative is that J. Edgar Hoover was a particularly power-hungry man, implying that with a different person in office, these surveillance abuses would not have happened. But the political spying wasn't a problem unique to Hoover. Presidents throughout the ages knew about FBI spying and took advantage of it. Theodore Roosevelt started the FBI to spy on anarchists.[35] Franklin Delano Roosevelt reinvigorated domestic political spying in the lead up to World War II.[36] And Lyndon Baines Johnson commanded the Central Intelligence Agency (CIA) to create a domestic surveillance operation, code named Chaos, in which the CIA and NSA eavesdropped on major peace groups.[37] Meanwhile, agencies other than the FBI were spying on Americans, too. Abusive surveillance did not die with Hoover and President Nixon.

The Snowden documents revealed that the NSA has developed plans to discredit people who hold politically radical beliefs. The NSA delves into its vast databases of Internet content and transactional data for information it can use to discredit those whom the agency believes are radicalizing others through speeches promoting disfavored—but not necessarily violent—political views. One report details vulnerabilities among its targets, such as viewing pornography, using donations for personal expenses, charging exorbitant speaking fees, or contradicting themselves in public. The document identifies six people and their areas of weakness, gleaned from surveillance. These targets were not necessarily criminals, violent, or even foreigners. In the document one of the six examples of people ripe for discrediting was an American.[38]

Some may say that the days of political spying are behind us. That is not the case. There are many documented examples of groups singled out for their religion or because of political beliefs. For domestic groups, rules often say that one may not be investigated "solely on the basis of activities protected by the first amendment to the Constitution of the United States."[39] Yet, it is not difficult to come up with another reason. The Civil Rights Movement was purported to have been directed by Soviet communists. Black Lives Matter is surveilled because law enforcement argues there may be violence at rallies organized by the group. The Trump administration justifies targeting Muslims on the grounds that citizens of certain countries can pose a higher national security risk.

If such abusive surveillance has been less prevalent in recent decades, it is thanks to the legal rules adopted in 1978, after congressional investigations of surveillance scandals of the 1960s and 1970s. But, since the attacks of September 11, those rules have been steadily neutered. At the same time, surveillance tools and capabilities have gotten far more powerful.

Americans must continue to be vigilant to ensure that our laws are impervious as possible to political abuses, because this is still a danger today. In December of 2015, for example, the statute that the intelligence community had been misinterpreting to justify bulk collection of domestic telephone call records was set to expire. The five-year expiration date had been built into the statute precisely because it was controversial, and legislators wanted to ensure that they would have to reconsider that grant of surveillance authority. The rare opportunity of expiration forced Congress to do something, and in a last minute showdown, it reformed the law to make clear that bulk collection of documents, tangible things, and metadata under that authority was not allowed. However, the reform legislation, the USA Freedom Act, did not alter the intelligence agencies' collection of the content Americans' international communications with targeted foreigners under section 702.

Problem Areas for Section 702

With the FISA Amendments Act, of which section 702 is a part, scheduled to expire, or sunset, on December 31, 2017, Americans and their elected representatives in Congress once again get a rare opportunity to define permissible surveillance. When Congress revisits section 702, it can make reforms in light of what we've learned from Snowden and the subsequent investigations. With that in mind, there are several key issues areas that call out the most for attention.

Protecting Online Communication and Storage of Personal Data and Effects

An overarching problem with foreign intelligence surveillance is the question of what data is considered "private" in the first place. Under U.S. law, there is no overarching right of privacy. Rather, statutes protect certain categories of data from collection or use. Under the Foreign Intelligence Surveillance Act, the government must get a foreign intelligence

warrant or comply with the more minimal protections of section 702 when it conducts "electronic surveillance" for foreign intelligence purposes. But other information-gathering practices that do not amount to "electronic surveillance" are not governed by FISA and don't receive FISA's protections.

Under FISA, there are four government activities that constitute "electronic surveillance." The definition of these categories is complicated, and depends, among other things, on the means of transmitting the communication, the location of government collection, and whether an American is known to be a party to the conversation. Importantly, the rules governing electronic surveillance generally only come into play when the government is invading a "reasonable expectation of privacy."

"Reasonable expectation of privacy" is a constitutional term. The Fourth Amendment prohibits unreasonable searches and seizures. While the phrase does not appear in the Fourth Amendment, case law has defined "search" as a government activity that invades a person's "reasonable expectation of privacy" in a place or in particular information. If the Fourth Amendment applies, then ordinarily the government activity requires a judicially issued warrant based on probable cause.

The "reasonable expectation of privacy" requirement is far narrower than one might think. In 1979, in *Smith v. Maryland*, the Supreme Court held that people have no "reasonable expectation of privacy" in the phone numbers we dial. To arrive at that conclusion, the Supreme Court harkened back to the days when callers would talk to a live operator and place calls by asking to be connected to a particular number, meaning information was knowingly and voluntarily disclosed to the phone company.[40] A few years earlier, in *United States v. Miller*, the Supreme Court had reasoned that a customer has no expectation of privacy in her bank records, because those are created by and managed by the financial institution.[41]

In the years since, the Department of Justice has relied on *Smith* and *Miller* to argue that—beyond phone numbers and bank records—if your information is exposed to any third party, then you do not have an expectation of privacy in it, and thus the government can get it without a warrant. In other words, if it isn't secret, then it isn't private. This notion has come to be known as the "third party doctrine."

Thanks to the third party doctrine, the Department of Justice does not believe that people have a reasonable expectation of privacy in phone calling records, Internet transactions, financial records, hard drive backups, or other sensitive data stored with "cloud" Internet services. If they are right, searches of personal data stored online is not protected by the Fourth Amendment. Further, FISA may not even apply, because the government activity does not fit the definitions of "electronic surveillance."

The expiration of the FISA Amendments Act is an opportunity to ensure that online information Internet users expect will remain private receives legal protection. Stored documents, location information, photographs, email, and online chats should receive privacy protection. Expanding the definition of electronic surveillance to ensure that collecting these kinds of data is covered by the statute would be a huge step toward protecting people from cavalier, opportunistic, and unnecessary government spying. The definitions of electronic surveillance activities should not depend on the Department of Justice's interpretation of this constitutional phrase "reasonable expectation of privacy." If the data is sensitive, if an American is a party to the conversation, or if the collection activity takes place inside the United States, FISA's privacy protections should apply. Congress could remove the "reasonable expectation of privacy" language from the statutory definition, and make clear that communications, personal documents, and metadata are protected by FISA.

The Broad Scope of Warrantless Wiretapping and Content Surveillance

Much of the policy debate over section 702 is centered on the provision's alleged national security or counterterrorism successes. This is surprising, because section 702 explicitly is not a counterterrorism statute, and is in fact much broader. Under section 702, surveillance can occur for any "foreign intelligence" purpose, including the collection of information about a foreign power or territory that is related to "the conduct of the foreign affairs of the United States." That includes eavesdropping on the heads of state, gathering information relevant to predicting the price of oil, and gaining leverage in negotiating trade disputes.

Intelligence officials reply that, while the statute allows surveillance for such broad purposes, the actual topics for which the community uses section 702 are more narrow. That is because in order to conduct surveillance under section 702, the government first must obtain a "certification" from the Foreign Intelligence Surveillance Court (FISC). The FISC is comprised of federal judges who make classified decisions on surveillance applications. One of these judges must approve a certification as a precursor to section 702 collection. Certifications identify categories of foreign intelligence information regarding which the U.S. Attorney General and the Director of National Intelligence authorize acquisition through the targeting of non-U.S. persons reasonably believed to be located abroad. Experts believe that these certifications are for gathering foreign intelligence information about foreign governments, counterterrorism, counterintelligence, and counterproliferation. There may also be a cybersecurity certification. Thus, the officials imply, section 702 surveillance only takes place for these important purposes. Therefore, section 702 does not have the broad impact on everyday foreigners that critics say.

It would be a mistake to put too much weight on the certifications as limiting section 702. Intelligence officials have not confirmed the subject matter of the certifications, and have never represented that these are or will remain the only certification topics. Nothing in the statute limits acceptable certifications to these national-security related topics. Any

foreign intelligence topic will do.[42] Nor does the FISC review any of the targeting decisions made under these certifications. Those decisions are within the discretion of the intelligence community.

As a result, average foreigners have legitimate concerns about being spied on even though they are neither terrorists nor agents of foreign powers. The statute allows these people to be targeted for being of foreign intelligence interest, even if they are not working for a foreign government, not engaged in terrorism, and not posing a threat to U.S. interests.

U.S. officials say that Americans should not be concerned with section 702 surveillance because it explicitly targets foreigners overseas, prohibits targeting U.S. persons, and also forbids "reverse targeting," a practice in which foreign targets are chosen with the ulterior motive of wiretapping Americans. However, Americans should not be reassured. Even when section 702 collection is about "foreign" intelligence, it does not only impact foreigners.

A recently declassified FISC opinion from November 2015 confirmed that section 702 actually sweeps up "substantial quantities" of information concerning U.S. persons.[43] Obviously, when an individual is a surveillance target, investigators will inevitably pick up conversations that person has with innocent third parties. Those third parties could include Americans. This makes sense. If you are talking to terrorists, agents will listen in. This collection is called "incidental" because it is incident to the permissible surveillance.

The difference is in the way the government treats these innocent conversations depending on whether it is a criminal investigation or an intelligence effort. In the criminal wiretap context, the agents have to minimize this eavesdropping by only listening to conversations about the criminal activity under investigation. For example, if investigating organized crime, the agents have to hang up the phone and not record when the suspects are talking to their parents or planning dinner for the evening.

But in the foreign intelligence context, agents gather everything they can about the target and then select interesting and relevant intelligence from the collected materials. Some agencies have access to the raw data and can search it for information—related and unrelated to the foreign intelligence topic for which it was collected. Other agencies have access to minimized data where Americans' identifying information has been blacked out, but it could be restored if need be.

Thus, the broader the surveillance of foreigners for general foreign intelligence purposes, the more Americans are spied on, too. Moreover, under section 702, the government is collecting international communications even when the foreign intelligence target is not a party to the conversation. Under Upstream collection, the government scans data flowing over the Internet for messages that contain particular selectors and thus are "about" the foreign intelligence target. Foreigners who are not targets are being spied on.

While incidental collection of information on Americans may be palatable for criminal or counterterrorism purposes, it is out of line for general foreign intelligence collection.

While incidental collection of information on Americans may be palatable for criminal or counterterrorism purposes, it is out of line for general foreign intelligence collection. Invading the privacy of Americans talking with foreigners targeted for their knowledge of topics such as trade disputes and the price of oil goes too far. Invading the privacy of Americans talking with foreigners about foreign intelligence targets is extreme. This is especially true because foreign intelligence targets are not only individuals, but organizations, too. Americans' communications with these organizations —the United Nations, Doctors Without Borders, and more—results in expansive impact on citizens.

Further, under the Upstream program, the NSA is collecting "Internet transactions" rather than discrete messages. An Internet transaction might contain multiple messages—the agency refers to this bundle of messages as a multi-communications transaction (MCT). An MCT could be something like your email inbox, which contains many, many messages. If only one email in your inbox is responsive to the NSA's targeting terms, the NSA collection system may nevertheless pull your entire inbox flow into the NSA databases. The collection of MCTs further removes the connection between the communicants and the intended target, because any communication that is embedded within a transaction that happens to include a communication that so much as mentions the targeted selector can get swept up.

The public is not fully aware of the scope of "abouts" collection. Much depends on what search terms, or "selectors," the agency chooses to use. While a search term theoretically could be as broad as "France" or "oil prices," the NSA says it does not use proper names like "Osama bin Laden" or "Petrobras" to conduct the surveillance. Rather, according to the intelligence agencies and the Privacy and Civil Liberties Oversight Board, section 702 selectors are "things like" email addresses, phone numbers, or Internet protocol addresses. Thus, if the target is Angela Merkel, intelligence officials say you'd need to have her email address and not just her name in your conversation in order for your messages to be collected.

Narrow selectors are a good thing. But, email addresses and IP addresses still can lead to very broad collection. If the NSA is acquiring messages sent to or from addresses like "membership@doctorswithoutborders.org" or "mailinglist@greenpeace.net," the incidental collection will be huge. Internet protocol addresses may be shared by many individuals or entities who are not themselves foreign intelligence targets.

In short, multiple people, none of whom is a target, may nevertheless be monitored because of the topic of their conversation, so long as one of the parties to the conversation is a foreigner located overseas.

What is particularly surprising for non-experts is that section 702 collection is not only about broad foreign intelligence interests. It can also be designed for criminal investigations, so long as a "significant purpose" of the collection is to obtain foreign intelligence information. In this way, section 702 gives a great amount of surveillance power to criminal investigators. Normally, if an FBI agent is investigating tax fraud or drug sales, she must get a wiretap warrant to eavesdrop on the suspect's conversations. That means showing probable cause to a judge, demonstrating that the surveillance was necessary, and complying with minimization and reporting procedures. With section 702, however, that agent can collaborate with an intelligence agent to wiretap the suspect with the intention of bringing criminal charges, so long as another significant reason for the wiretapping is intelligence gathering.

Not only does section 702 enable surveillance about a broad swath of topics, it is also loose about who may be targeted. In the criminal context, courts ensure that people who are wiretapped are the right people. This oversight serves two purposes. It makes agents explain the reasons for believing that watching the target will reveal information to which the government is entitled. It also gives a presumably neutral and detached person—the judge—the ability to weigh in on, and ultimately to narrow or to veto the government's targeting decision. In contrast, under section 702, no judge participates in the government's targeting decisions. Courts assess whether the targeting procedures fit the statutory definition of targeting procedures, but they do not oversee targeting decisions.[44] Rather, the ultimate decision about who intelligence authorities spy on is entirely an internal determination.

Judicial review is an important check on surveillance power. Without it, improper or ill-advised surveillance is far more likely. For example, the public recently learned that the NSA targeted a peaceful New Zealand pro-democracy activist under the PRISM surveillance program based on erroneous claims by the New Zealand government that the man was plotting violent attacks.[45] Had the NSA been required to provide some factual justification to a judge, the surveillance (in which the agency captured communications of people associated with a Fijian "thumbs up for democracy" campaign and turned them over to the New Zealand government) might not have happened.

Wiretapping innocent people is nothing new or surprising. It routinely happens when suspects talk to their friends, family and coworkers. But it takes on a new scope under section 702. Because the authorized topics of surveillance are so broad, because there is no judicial oversight of target selection, because technology makes comprehensive information collection and storage possible and cheap, section 702 has a disproportionate impact on American privacy.

Congress could limit this impact by restricting section 702 collection to matters of national security concern, such as terrorism, proliferation of weapons of mass destruction, attacks by foreign powers, and counterintelligence activities. There will still be substantial warrantless wiretapping of Americans, but at least narrowing the scope of surveillance would be in service of national security. Counterterrorism experts have endorsed similar reforms. In December of 2013, President Obama convened a review group on intelligence and communications technologies to advise on issues raised by the ongoing Snowden revelations. The review group included Richard A. Clarke, former national coordinator for security, infrastructure protection and counter-terrorism for the United States, as well as Michael J. Morell, a former acting Central Intelligence Agency director. The other three members were law professor Geoffrey Stone, former administrator of the White House Office of Information and Regulatory Affairs Cass Sunstein, and former chief counselor for privacy in the Office of Management and Budget Peter Swire. The five recommended that, as a general rule, the government should not be permitted to collect and store raw personal information about individuals, whether for foreign intelligence or law enforcement purposes.[46] Rather, government collection or storage of private data must be "narrowly tailored to serve an important government interest." Specifically, section 702 "must be directed exclusively at the national security of the United States or our allies." Anything less means vast amounts of private information in government hands—a real danger for abuse. This recommendation fits well with human rights law which requires surveillance activities to be "necessary and proportionate."[47]

If Congress limited section 702 collection to national security topics, it would more closely tie the collection to matters critical for the United States. More general foreign intelligence gathering inside U.S. borders would continue, but under traditional Foreign Intelligence Surveillance Act provisions, which require that the government have probable cause to believe that the target is an agent of a foreign power, for example, working with a foreign terrorist group.

Another approach would be for Congress to end Upstream collection entirely. Upstream is extremely invasive. It is the program that over-collects MCTs containing irrelevant information, and it entails "abouts" collection, gathering non-targets' communications if the parties are communicating about targeted selectors. It also entails scanning every message that flows through particular network switches, constituting a dragnet search through (at least) Americans' international communications.[48] Dragnet scanning and collection of irrelevant messages and messages about foreign intelligence targets may well be unconstitutional under the Fourth Amendment, which prohibits unreasonable searches and seizures. The NSA would likely continue to maintain its scanning capabilities at various Internet chokepoints because the secretive FISA court has given it the authority to conduct surveillance of communications between foreigners that flow over U.S. networks under its transit authority. But it would have to shut off the filters that search and gather conversations where one of the participants is an American.

The Retention and Usage of Collected Information

Limiting collected information to important national security purposes is the best way to protect people from government abuse of the data. Reducing data intake alone, however, cannot constrain abuse. Post-collection usage rules are necessary for effective reform. The retention, analysis, and sharing of section 702 data is governed by internal, changeable, and frequently classified, "minimization procedures" that a FISA judge reviews, but has little power to veto or modify.

According to these rules, the NSA is limited to looking for foreign intelligence information and restricted in searching for information about Americans, in accordance with its mission as a foreign intelligence agency. In fact, the NSA and the CIA minimization procedures now require analysts to create a "statement of facts showing that a query is reasonably likely to return foreign intelligence information" before searching section 702 data for U.S.-person information, but the procedures do not require that foreign intelligence be the purpose of conducting the search.[49]

But the FBI is a domestic intelligence and law enforcement agency, and it has powerful access to this information. Recall that foreign intelligence only has to be a significant purpose of the collection for its gathering to proceed, meaning the FBI's criminal investigation interests can be paramount. The same is true, but more importantly so, with subsequent use of the collected data.

The FBI has access to raw PRISM data from the NSA. Once the data is collected and retained, agents can trawl through the database of calls and messages, looking for information not only about foreign intelligence but also criminal activity. They can look for Americans in this trove of data, effectively circumventing the need to get a search warrant based on probable cause from a judge—a practice known as "backdoor searching."

Backdoor searching is possible because minimization procedures allow FBI agents to query 702-acquired data for U.S.-person information as part of routine criminal assessments or investigations. The FBI doesn't need to show probable cause and get a search warrant for these searches, even though it would to gather the information on its own. In fact, the FBI can search section 702 data for U.S.-person identifiers in order to initiate an investigation—without any suspicion of wrongdoing. They do this routinely as part of "assessments," which require no factual predicate.[50] In other words, agents can search data for any routine law enforcement purpose.

Further, even agents who are not trained in how to handle section 702 data are allowed to search it and see the results. They just need an appropriately cleared agent to agree that the information either reasonably appears to be foreign intelligence information, is necessary to understand foreign intelligence information, or is evidence of a crime.[51] In this way, the FBI piggybacks on the NSA's foreign intelligence- and national security-justified collection to get warrantless access to Americans' private information.

There's a general concern about over-policing when cops are allowed to fish through vast repositories of private data looking for wrongdoing. For example, medical marijuana prescriptions are increasingly legal in many states, but illegal under federal law. Federal authorities could lawfully search the 702 databases looking for information about doctors issuing these prescriptions, and their patients. Databases of raw intercepts contain names and identifying information that could be abused to go after political or personal enemies. These tools are of extra concern today. Donald J. Trump has said that during the course of his presidency he wants to prosecute political challengers,[52] potentially create a database of Muslims inside the country,[53] and rapidly deport millions of people.[54] Furthermore, his attorney general, Jeff Sessions, has hinted at a crackdown on marijuana use, which could be used as a means to pursue arrests.[55]

Usage and retention rules need to minimize the capability for abuse. The President's Review Group recommended that information about any United States person should be purged from databases upon detection, "unless it either has foreign intelligence value or is necessary to prevent serious harm to others."[56] Further, the information should be limited to intelligence purposes, and not be used as evidence in criminal cases. Finally, if the government does want to search the database of section 702 for communications of particular United States persons, it should only be allowed to do so "(a) when the information is necessary to prevent a threat of death or serious bodily harm, or (b) when the government obtains a warrant based on probable cause to believe that the United States person is planning or is engaged in acts of international terrorism."[57]

National security provisions shouldn't be an end run around rules that require good cause and judicial oversight for regular investigations.

In other words, national security provisions shouldn't be an end run around rules that require good cause and judicial oversight for regular investigations. If you collect for national security, you use for national security, and nothing else.

In addition to restricting the scope of collection, Congress or the courts could restrict the use to which the information is put. The FBI's access to raw data should be cut off. FBI access to data would be limited to only those circumstances where the NSA analysts seek to share data for national security purposes or to prevent serious crimes. This change would ensure that the exceptional access our law permits to the NSA is not repurposed by the FBI.

At the very least, Congress should end the practice of "backdoor searching" for Americans' data. The only way to avoid abuse is for a judge to assess whether there is probable cause for the search before allowing it. Two members of the Privacy and Civil Liberties Oversight Board have recommended that a FISC judge review and approve identifiers before they may be used to query data collected under section 702 for a foreign intelligence purpose, other than in exigent circumstances or where otherwise required by law.[58] A regular judge in the public court system could also assess probable cause and issue warrants for searches intended to find evidence in criminal cases. Given the scope of U.S. criminal law, there will likely be something suspicious in the database about everyone. But requiring a warrant would help avoid suspicionless fishing expeditions motivated by curiosity or politics.

Balancing Secrecy and Accountability

Lack of accountability is perhaps the biggest systemic problem in surveillance. The central cause for this lack of accountability is that modern surveillance depends on an untenable level of secrecy. Spy agencies have always protected legitimate secrets—methods of surveillance, identity of agents, information gathered—from the targets. But now, in a society awash in information and a world where terrorists hide among the innocent, everyone's data is potentially subject to surveillance. As a result, modern surveillance is being hidden from everyone. This culture of secrecy has led to a proliferation of secret court opinions, classified policies, misleading use of language, aggressive prosecution of whistleblowers, spying on journalists, and suppressing court challenges.

In the dark, illegality and misconduct fester. The activities of American spies remain hidden from public oversight. The tools we have for checks and balances within the system also fail to deliver. Without public demand and expert debate, opportunities for reform are utterly cut off—no one knows what changes need to be made.

In response to the Snowden disclosures, the intelligence community has recognized that it needs to communicate more effectively with the public. This is in part so that the public understands the safeguards that do exist in limiting surveillance. For example, NSA officials have assured the public that "all three branches of government are involved" in approving and overseeing domestic spying.[59] Robert Litt, general counsel in the Office of the Director of National Intelligence (ODNI), says that there is extensive oversight and meaningful limitations on how information about Americans can be used.[60] The Civil Liberties Protection Officer in the ODNI, Alex Joel,says that "oversight is extensive and multi-layered." Joel identifies various legal offices, Inspectors general, and civil liberties committees that allegedly ensure that the intelligence agencies do not run amok.[61]

The oversight mechanisms are important. They help protect against insider abuse. Internal oversight can catch people breaking the rules to spy on their former spouses. Documenting database queries can expose agents who are improperly stalking their ex-lovers.

Existing oversight mechanisms are geared to catch unauthorized, individual violations of official policy. But they do not provide enough transparency to permit the public—or even courts and Congress—to participate in democratic decision making about whether the rules themselves are appropriate and balanced. Internal oversight alone is a poor way to figure out whether surveillance programs are a good idea. An emphasis on compliance rather than crafting balanced policies is a real problem in an area like surveillance where our technological capabilities have so outpaced the development of legal doctrine. Law is lagging behind, and surveillance overseers can let spying practices expand in the gaps without violating the "rule of law."

Nor are the oversight mechanisms well-designed to expose or correct a wayward president who has ordered illegal spying contrary to the rules. The offices that officials such as Joel and Litt point to as conducting oversight are mostly part of the executive branch, the same branch that American spies belong to. Internal oversight by its very nature has limited capacity to keep the executive branch itself in line. If the president, or the heads of the FBI, the Central Intelligence Agency (CIA), or the NSA decide on high to abuse surveillance powers, internal oversight is not a strong bulwark. The executive branch officials conducting the oversight ultimately report to the very same bosses who are ordering and conducting the surveillance activities they are supposed to oversee. That leaves the officials with difficult choices; stay and accept that the official policy is problematic or illegal, or quit. Keep quiet, or inform Congress, courts, or even the public.

The United States needs far more transparency and declassification about surveillance policies and practices. The public should demand that all judicial opinions on section 702 quickly be declassified and released with only minimal redactions. Currently, the intelligence community has been picking and choosing which opinions to release, thereby controlling what people know about surveillance laws and sculpting public opinion. This gamesmanship is unacceptable. The opinions should be released across the board.

The executive branch should also declassify and disclose more Office of Legal Counsel (OLC) opinions. OLC opinions tell the story of how the executive branch over time uses the law to build, or to limit, the national security state. These opinions show what the laws Congress passes and the rulings courts issue actually mean to American spies. Given the power of these opinions to both authorize surveillance and immunize officials, the public needs to know what those opinions say.

Conclusion

Foreign intelligence surveillance is an important part of U.S. national security. But the practice has, in secret, metastasized to the point where it is ripe for anti-democratic abuse. Fixing this problem can start with reforming section 702 when it comes up for renewal or sunset at the end of 2017.

1. Congress should consider amendments that would address the areas of section 702 that are most ripe for abuse, specifically the scope of collection, its retention and use, and the secrecy surrounding it.

2. Congress should consider whether to limit to national security interests the purposes for which the intelligence and law enforcement communities can conduct section 702 surveillance and use the resulting information;

3. Congress should consider how to protect Americans' communications from surveillance without a search warrant;

4. Congress should protect Americans from indiscriminate searches of communications content; and

5. Congress should consider how to support greater transparency and public oversight, for example by declassifying court opinions and internal memoranda that explain how section 702.

Right now, section 702 legitimizes programs that endanger civil liberties, but it doesn't need to be that way. The coming public debate over the provision can generate much needed democracy-friendly reforms.

Notes

1. Glenn Greenwald, "XKeyscore: NSA tool collects 'nearly everything a user does on the internet,'" *The Guardian*, July 31, 2013, https://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data.
2. 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_story.html?utm_term=.f2ec866443fc.
3. Sean Gallagher, "How the NSA's MUSCULAR tapped Google's and Yahoo's private networks," *Ars Technica,* October 31, 2013, https://arstechnica.com/information-technology/2013/10/how-the-nsas-muscular-tapped-googles-and-yahoos-private-networks/.
4. James Ball and Nick Hopkins, "GCHQ and NSA targeted charities, Germans, Israeli PM and EU chief," *The Guardian*, December 20, 2013, https://www.theguardian.com/uk-news/2013/dec/20/gchq-targeted-aid-agencies-german-government-eu-commissioner.

5. J. Granick, *American Spies: Modern Surveillance, Why You Should Care, and What To Do About It* (New York: Cambridge University Press, 2017).

6. Barton Gellman, "How 160,000 intercepted communications led to our latest NSA story," *Washington Post*, July 11, 2014. https://www.washingtonpost.com/world/national-security/your-questions-answered-about-the-posts-recent-investigation-of-nsa-surveillance/2014/07/11/43d743e6-0908-11e4-8a6a-19355c7e870a_story.html?utm_term=.3d020ebb0aee.

7. H.R. Rep. 112-645, August 2, 2012, 3. Section 702 information "is often unique, unavailable from any other source, and regularly provides critically important insights and operationally actionable intelligence on terrorists and foreign intelligence targets around the world"; Privacy and Civil Liberties Oversight Board, *Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act* (PCLOB Report), July 2, 2014, 108

8. Nicholas Niarchos, "Has the NSA Wiretapping Violating Attorney-Client Privilege?" *The Nation*, February 4, 2014, https://www.thenation.com/article/has-nsa-wiretapping-violated-attorney-client-privilege/.

9. NSA 2015 Minimization Procedures at § 6(a)(1)(a); CIA 2015 Minimization Procedures at 3.c; FBI 2015 Minimization Procedures at III.G.5.

10. Andrea Peterson "LOVEINT: When NSA officers use their spying power on love interests," *Washington Post*, August 24, 2013, https://www.washingtonpost.com/news/the-switch/wp/2013/08/24/loveint-when-nsa-officers-use-their-spying-power-on-love-interests/?utm_term=.62264cd38efb.

11. K. Devlin, "The NSA: A betrayal of trust," *Notices of the American Mathematical Society* 61 (June/July, 2014): 624–26.

12. Peter Maass, "Inside NSA, Officials Privately Criticize 'Collect It All' Surveillance," The Intercept, May 28, 2015, https://theintercept.com/2015/05/28/nsa-officials-privately-criticize-collect-it-all-surveillance/.

13. See W. Seltzer and M. Anderson. "After Pearl Harbor: The Proper Role of Population Data Systems in Time of War," Paper presented at the Population Association of America Annual Meeting, Los Angeles, CA, March 23–25, 2000, pantherfile.uwm.edu/margo/www/ govstat/newpaa.pdf.

14. T. Weiner, *Enemies: A History of the FBI* (New York: Random House, 2013), 57. FBI Director Burns worked with the Harding White House Attorney General in 1923 to spy on and drum up charges against two senators investigating corruption in the Administration.

15. FBI Special Agent Arthur Murtagh testimony before the House Select Committee on Intelligence, p. 1068. Hoover's deputy Cartha DeLoach said that a Senator had caught driving drunk with a "good looking broad." The senator was made "aware that we had the information, and we never had trouble with him on appropriations since."

16. Beverly Gage, "What an Uncensored Letter to M.L.K. Reveals," *New York Times*, November 11, 2014, https://www.nytimes.com/2014/11/16/magazine/what-an-uncensored-letter-to-mlk-reveals.html.

17. A. Neier, "Spying on Americans: A very old story," *New York Review of Books*, June 18, 2013, www.nybooks.com/blogs/nyrblog/2013/jun/18/ spying-americans-very-old-story/.

18. R. Shilts, *Conduct Unbecoming: Gays & Lesbians in the U.S. Military* (New York: Open Road Media, 1996), relating the experience of Air Force Sgt. Dan Bell.

19. Colin Moynihan, "A New York City Settlement on Surveillance of Muslims," *The New Yorker*, January 7, 2016,

http://www.newyorker.com/news/news-desk/a-new-york-city-settlement-on-surveillance-of-muslims.

20. 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.

21. 50 U.S.C. 1881a.

22. 50 U.S.C. 1881a (g)(2)(A)(iv).

23. See Privacy and Civil Liberties Oversight Board (PCLOB),*Report on the Surveillance Programs Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act*, July 2, 2014, [hereinafter "PCLOB Report"] at 24–25.

24. Ibid., 25

25. 50 U.S.C. § 1801(e)(2)(B) (emphasis added). For information concerning U.S. persons, the information must be "necessary to," rather than "relate to." Id.

26. [Redacted], Docket [Redacted], at *27 n.25 (FISC Nov. 6, 2015) [hereinafter "Hogan Opinion"], available at https://www.dni.gov/files/documents/20151106-702Mem_Opinion_Order_for_Public_Release.pdf.

27. As David Medine, former chairman of the PCLOB, said during the May 10 Senate Judiciary hearing, "this program targets anyone with foreign intelligence value. It could be a completely innocent businessman or anyone else out of the country who has that information." See *Hearing Before the S. Comm. On the Judiciary* 114th Cong. (May 10, 2016),*supra* n.1.

28. PCLOB Report.

29. Granick, *American Spies*, 119.

30. Dustin Volz, "U.S. to disclose estimate of surveilled Americans by early 2017," Reuters, December 16, 2016, http://www.reuters.com/article/usa-cyber-surveillance-idUSL1N1EA2DE.

31. B. Gellman, J. Tate, and A. Soltani, "In NSA-intercepted data, those not targeted far outnumber the foreigners who are," *Washington Post*, July 5, 2014,https://www.washingtonpost.com/world/national-security/in-nsa-intercepted-data-those-not-targeted-far-outnumber-the-foreigners-who-are/2014/07/05/8139adf8-045a-11e4-8572-4b1b969b6322_story.html.

32. Ibid.

33. Dustin Volz, "NSA contractor indicted over mammoth theft of classified data," Reuters, February 8, 2017, http://www.reuters.com/article/us-usa-cybersecurity-nsa-contractor-idUSKBN15N2N4.

34. Barton Gellman, Julie Tate, and Ashkan Soltani, "In NSA-intercepted data, those not targeted far outnumber the foreigners who are," *Washington Post*, July 5, 2014,https://www.washingtonpost.com/world/national-security/in-nsa-intercepted-data-those-not-targeted-far-outnumber-the-foreigners-who-are/2014/07/05/8139adf8-045a-11e4-8572-4b1b969b6322_story.html?utm_term=.979d6c835d4b&wpisrc=al_national.

35. Weiner, Enemies, 11.

36. Ibid., 86–89.

37. T. Weiner, *Legacy of Ashes: The History of the CIA*(New York: Anchor Books, 2008), 329.

38. Jennifer Granick, "NSA SEXINT is the Abuse You've All Been Waiting For,"*Just Security*, November 29, 2013, https://www.justsecurity.org/?p=3918/.

39. *See e.g*. 50 U.S.C. §§ 1805(a)(2)(A), 1824(a)(2)(A), 1843, 1861.

40. *Smith v. Maryland*, 442 U.S. 735 (1979).

41. *United States v. Miller*, 425 U.S. 435 (1976).

42. 50 U.S.C. 1881a(g).

43. Hogan Opinion, 27 n.25.

44. PCLOB Report, 25.

45. Ryan Gallagher and Nicky Hager, "The Raid: In Bungled Spying Operation, NSA Targeted Pro-Democracy Campaigner," *The Intercept*, August 14, 2016,https://theintercept.com/2016/08/14/nsa-gcsb-prism-surveillance-fullman-fiji/.

46. The President's Review Group on Intelligence and Communications Technology,*The NSA Report: Liberty and Security in a Changing World* (Princeton, N.J.: Princeton University Press, 2014), https://books.google.com/books/about/The_NSA_Report.html?id=XkClAgAAQBAJ.

47. Universal Declaration of Human Rights Article 29; General Comment No. 27, Adopted by The Human Rights Committee Under Article 40, Paragraph 4, of the International Covenant on Civil and Political Rights, CCPR/C/21/Rev.1/Add.9, November 2, 1999.

48. PCLOB Report, 37.

49. A new policy announced by the administration in February 2015 required a "written statement" of facts. See Office of the Director of National Intelligence, "New Privacy Protections for Information Collected Under Section 702," IC ON THE RECORD, February 3, 2015, https://icontherecord.tumblr.com/ppd-28/2015/privacy-civil-liberties. The newly-declassified 2015 minimization procedures (which were approved in July 2015) merely require a "statement of facts," without specifying that a written version is required. See NSA 2015 Minimization Procedures § 3(b)(5); CIA 2015 Minimization Procedures § 4. However, in order to comply with the DOJ and ODNI's oversight requirements, the NSA must submit a list of all U.S.-person identifiers approved to be used to query section 702 data, along with information detailing why those identifiers are reasonably likely to return foreign intelligence information. The CIA must submit a list of every section 702 query using a U.S.-person identifier, as well as a "contemporaneously written" justification regarding why those identifiers were reasonably likely to return foreign intelligence information. See Office of the Director of National Intelligence, "Release of a Summary of DOJ and ODNI Oversight of Section 702," IC ON THE RECORD 3–4 (released August 11, 2016), https://icontherecord.tumblr.com/post/148796781888/release-of-a-summary-of-doj-and-odni-oversight-of .

50. FBI Domestic Investigations and Operations Guide §5.1.

51. Hogan Opinion, 35.

52. Yoni Appelbaum, "Trump's Promise to Jail Clinton Is a Threat to American Democracy,"*The Atlantic*, October 10, 2016, https://www.theatlantic.com/politics/archive/2016/10/trumps-promise-to-jail-clinton-is-a-threat-to-american-democracy/503516/.

53. Lauren Carroll, "In Context: Donald Trump's comments on a database of American Muslims,"*Politifact*, November 24, 2015. http://www.politifact.com/truth-o-meter/article/2015/nov/24/donald-trumps-comments-database-american-muslims/.

54. Julie Hirschfeld Davis and Julia Preston, "What Donald Trump's Vow to Deport Up to 3 Million Immigrants Would Mean," *New York Times*, November 14, 2016,https://www.nytimes.com/2016/11/15/us/politics/donald-trump-deport-

immigrants.html.

55. Tessa Berenson, “Attorney General Jeff Sessions Just Hinted at a Crackdown on Legal Marijuana,”*Time*, February 28, 2017, http://time.com/4685414/jeff-sessions-recreational-marijuana-legal-crackdow/.

56. The President’s Review Group on Intelligence and Communications Technology,*The NSA Report: Liberty and Security in a Changing World* (Princeton, N.J.: Princeton University Press, 2014), Recommendation 12, 28–29, https://books.google.com/books/about/The_NSA_Report.html?id=XkClAgAAQBAJ.

57. Ibid.

58. PCLOB Report, Annex A, Separate Statement of Chairman David Medine and Board Member Patricia Wald, pp. 151–52.

59. *Hearing of the House Judiciary Committee on Oversight of the Administration’s Use of the Foreign Intelligence Surveillance Act (FISA) Authorities*, July 17, 2013, testimony of James Cole, Deputy Attorney General, U.S. Department of Justice,

Robert Litt, General Counsel, Office of Director of National Intelligence,

https://icontherecord.tumblr.com/post/57804306650/hearing-of-the-house-judiciary-committee-on.

60. See e.g. ODNI General Counsel Robert Litt’s As Prepared Remarks on Signals Intelligence Reform at the Brookings Institute, Tuesday, February 10, 2015, available at https://www.dni.gov/index.php/newsroom/speeches-and-interviews/208-speeches-interviews-2015/1171-odni-general-counsel-robert-litt%E2%80%99s-as-prepared-remarks-on-signals-intelligence-reform-at-the-brookings-institute?highlight=WyJzZWFyY2giXQ==.

61. Alexander W. Joel, “The Truth About Executive Order 12333,”*Politico*, August 18, 2014, http://www.politico.com/magazine/story/2014/08/the-truth-about-executive-order-12333-110121.

Jennifer Granick, Contributor

Jennifer Stisa Granick is the Director of Civil Liberties at the Stanford Center for Internet and Society. She is the author of a new book from Cambridge University Press, American Spies: Modern Surveillance, Why You Should Care, and What To Do About It.