A HOOVER INSTITUTION ESSAY

Go Big, Go Global

SUBJECT THE NSA'S OVERSEAS PROGRAMS TO JUDICIAL REVIEW

TIMOTHY H. EDGAR

Series Paper No. 1605

The United States should stop being defensive about surveillance. America leads the world when it comes to rules to protect privacy in intelligence surveillance—if only because the rest of the world's rules are so weak. Under the Foreign Intelligence Surveillance Act of 1978, a court must review electronic surveillance for intelligence purposes where the surveillance takes place in the United States, targets people in the United States, or targets American citizens or residents anywhere in the world. For all intelligence activities, including the signals intelligence activities of the National Security Agency, Executive Order 12,333 requires rules to protect the privacy of American citizens and residents. President Obama has extended some of these protections to foreigners, anywhere in the world. There is a robust system of intelligence oversight to enforce these rules. It includes offices of general counsel, inspectors general, civil liberties and privacy offices, outside privacy and oversight boards, and review by congressional intelligence and judiciary committees. Most democratic countries do not have anything like these rules and institutions for protecting privacy in intelligence surveillance.

Nevertheless, these rules, including FISA, were primarily designed in and for a different era, before globalization and the Internet—an era of international telegrams, analog telephones, and conflict between rival superpowers. The basic premise of FISA is that surveillance programs inside the United States pose significant civil liberties issues requiring judicial review, while the issues posed by global surveillance programs should be left to the executive branch. In the late 1970s, that premise made sense. International travel and communication were exotic and expensive. After September 11, 2001, Congress expanded surveillance powers and amended provisions of FISA that had posed barriers to information sharing.[1] These changes did not challenge the basic divide at the heart of FISA between domestic national security surveillance and global signals intelligence.

In 2008, Congress enacted section 702 of FISA. Section 702 authorizes collection of foreign intelligence inside the United States, so long as the direct targets of surveillance are foreign citizens located outside the United States. As section 702 involves domestic collection of data and communications, it was seen at the time as another expansion of surveillance powers during the George W. Bush administration, justified (fairly or unfairly) by the need to combat international terrorism. In fact, section 702 has proved a valuable tool for collecting intelligence on international terrorism and other transnational threats, although it allows surveillance for much broader intelligence purposes.[2]

Section 702 expires at the end of 2017. The debate over reauthorizing it has begun. Supporters argue the law is vital, protects civil liberties, and should be extended without change. Civil liberties, privacy, and human rights advocates urge its expiration or, at a minimum, significant reforms. These include greater transparency about how often the NSA collects communications of Americans alongside those of foreigners. Advocates also urge tighter controls on queries of section 702 using identifiers belonging to Americans (so-called "backdoor searches"). In addition, they want an end to the use of section 702 to scan the Internet backbone ("upstream collection") and a ban on the collection of communications that include identifiers of a foreign target, but are not to or from that target ("about collection"). Finally, American communications providers and Internet companies warn of the economic consequences of section 702, including lost business from foreign customers.[3]

While these concerns have some merit, it is a mistake for civil libertarians to view section 702 in an exclusively negative light. Section 702 is the first provision of FISA specifically intended by Congress to provide judicial review of broad programs of signals intelligence collection that do not intentionally target American citizens or residents or anyone inside the United States. As such, section 702 sets a positive example, albeit an ambiguous one, of subjecting the NSA's global surveillance to review by all three branches of government.

The most important thing that Congress and the next president should do in next year's debate over section 702 is to broaden the conversation. The continuing fallout over Edward Snowden shows that global surveillance has touched a nerve in an interconnected world.[4] A narrow focus on reforming section 702 and the programs it authorizes would be a missed opportunity for civil liberties, privacy, and human rights. In the Internet age, it is no longer desirable or even possible to protect the privacy of Americans while leaving the rules for most global surveillance programs entirely to the executive branch.

Congress should use the debate over section 702 to think big. In 2017, Congress should bring the NSA's global surveillance out of the shadows and under a legal framework that is designed for this century. Comprehensive reform would include three steps:

- First, with a few specific exceptions outlined below, all NSA surveillance programs should be subject to FISA. The experience of section 702 shows that judicial review of global surveillance is feasible while preserving the effectiveness of signals intelligence. NSA surveillance should be subject to statutory limits and court review regardless of where and how data is collected and regardless of the nationality of the direct targets of surveillance.

- Second, judicial review provides a way for the United States to limit surveillance of the citizens of some countries to international terrorism and other specific security threats.

Limits could apply to citizens of friendly democratic countries if—and only if—their governments agreed to limit their intelligence practices on a reciprocal basis and subject them to meaningful oversight, such as court review. Section 702 shows that courts can provide the effective limits on surveillance programs that would make such an arrangement credible and enforceable.

- Finally, Congress should provide that signals intelligence programs be subject to meaningful challenge in the federal courts by those who reasonably fear surveillance, even if they cannot show their communications have actually been intercepted. Section 702 demonstrates that courts are capable of providing meaningful review to enforce constitutional guarantees, while accommodating the government's requirements of flexibility, speed, and secrecy when it comes to complex intelligence collection programs.

This three-part plan for comprehensive NSA reform is radical in conception. It subjects to scrutiny by Congress and the federal courts global surveillance programs that have previously avoided congressional and judicial oversight. Nevertheless, the experience of section 702 shows that reform can be implemented in a manner that would be modest in its practical impact on the operations and effectiveness of the NSA and other intelligence agencies.

The United States has a robust tradition of constitutional checks and balances, along with substantial experience with adapting those checks and balances to intelligence surveillance. In 1978, Congress passed FISA, which for the first time subjected national security wiretapping to judicial review. In 2008, Congress passed amendments to FISA that brought broad NSA programs directed at foreign targets under judicial review. Court oversight gives teeth to rules designed to prevent abuse. In both 1978 and 2008, there were fears the new requirements would overburden the intelligence community or impair its effectiveness. They proved overblown. This experience uniquely positions the United States for a leadership role. The United States already leads the world in mass surveillance. It should lead the world in mass surveillance reform.

Step 1: Subject global surveillance programs to review by the Foreign Intelligence Surveillance Court.

Today, the Foreign Intelligence Surveillance Act of 1978 subjects some intelligence surveillance—surveillance that intentionally targets Americans, or where collection is from a switch or a server on US soil—to independent review, involving all three branches of government. All other intelligence surveillance, including the NSA's collection of satellite communications and essentially all of its collection overseas, whether directly or through allied intelligence services, is governed only by Executive Order 12,333. Part 2 of E.O. 12,333 requires rules to protect the privacy of US persons: American citizens and

permanent residents, along with US corporations and organizations composed substantially of US persons. Under Presidential Policy Directive 28 (PPD-28), issued in January 2014, the NSA's rules for US persons have been supplemented by guidelines that provide modest protection for the privacy of foreign citizens.[5] Unlike collection under FISA, both the rules for US persons and the guidelines required by PPD-28 are administered entirely within the executive branch.

The rules and institutions that FISA and E.O. 12,333 create—and the dividing line between these two regimes for protecting privacy and civil liberties—were the result of investigations of intelligence activities during the 1970s. The most significant was the Senate committee chaired by Frank Church of Idaho. As it concerned electronic surveillance, Senator Church's investigation focused primarily on the FBI wiretapping and on two NSA programs, Shamrock and Minaret, which clearly involved spying on Americans.[6]

During its investigations, Congress was told about NSA listening posts around the world and inside the United States that were scooping up a vast quantity of communications from satellites. Satellites were the dominant technology for international telecommunications at that time, although such technology was also used for long-haul domestic communications. In 1975, Church explained in a media interview, "The United States government has perfected a technological capability that enables us to monitor the messages that go through the air." Church warned that this "capability at any time could be turned around on the American people, and no American would have any privacy left, such is the capability to monitor everything—telephone conversations, telegrams, it doesn't matter. There would be no place to hide."[7] In the same interview, Church accepted that these NSA surveillance capabilities were "necessary and important to the United States as we look abroad at enemies or potential enemies." NSA critics often omit this acknowledgement. Glenn Greenwald carefully excises these words when he quotes Church at the beginning of his book about the Snowden revelations, *No Place to Hide*.[8]

While FISA was intended to prevent the NSA from using its global signals intelligence capabilities to spy on Americans, it was also written to preserve those capabilities for spying on foreigners. Congress did this by intentionally exempting most of what the NSA does from the new court it created to review national security wiretapping, so long as the NSA did not target US persons on purpose. In FISA, Congress defined "electronic surveillance" to include four sets of activities it intended to bring within the court's purview:

1. Collection of communications from signals in the air, if the government intentionally targets a "particular, known" US person inside the United States.

2. Collection of communications while they travel on a wire (including a switch or server) inside the United States, if any party to the communication is in the United States.

3. Collection of wholly domestic communications.

4. The installation of a bugging device inside the United States where "a person has a reasonable expectation of privacy" and a warrant would normally be required.[9]

This definition does not prevent the NSA from using its listening posts inside the United States to collect signals over the air, provided that the NSA does not intentionally target a US person. Likewise, it does not cover the NSA's overseas collection of communications, so long as no US person is intentionally targeted. For collection inside the United States that is not from the air—such as collection from the international gateways of undersea cables, with the assistance of American telecommunications companies—Congress adopted a more restrictive rule, outlined in the second paragraph of the definition. It forecloses the collection of communications content if there is any possibility some communications may include a party who is inside the United States. In theory, the rule permits collection of transiting foreign-to-foreign communications: communications that travel on a wire through the United States as they go from one foreign person outside the United States to another foreign person outside the United States. However, the NSA does not collect individual communications, whether foreign-to-US or foreign-to-foreign. Instead, it collects all the communications that include a selector, such as a telephone number or e-mail address, associated with a particular target. Because the NSA cannot predict in advance of collection whether one of its targets overseas will or will not communicate with a person inside the United States, as a practical matter the second paragraph of the definition of electronic surveillance in FISA forecloses almost all collection from a wire or switch inside the United States without a court order.

During the decades following the enactment of FISA, technology and society changed dramatically. While the NSA continues to collect signals from the air, most of the world's communications, telephone and Internet, now travel as digital packets, usually by fiber-optic undersea cable rather than by satellite. Communications of foreign persons outside the United States transit the international gateways inside the United States that sit along the Internet backbone. Internet communications may reside on servers maintained by companies inside the United States, even where the account holder is a foreign person residing overseas. Prior to the enactment of section 702, the government could obtain such communications under FISA only with an individual court order, based on a probable cause that the target is a foreign power or an agent of a foreign power—the same standard that applies to domestic national security wiretaps. Alternatively, it could violate FISA—as it did, secretly, during the George W. Bush administration from 2001 to 2007 as part of the NSA's Stellarwind program.[10]

When Congress enacted the Protect America Act in 2007, and its successor, section 702 of FISA, supporters argued these laws simply updated FISA to reflect these changes in communications technology. Section 702 permits the government to obtain orders

from the Foreign Intelligence Surveillance Court requiring electronic communications service providers to cooperate with surveillance of "persons reasonably believed to be located outside the United States to acquire foreign intelligence information." In passing section 702, Congress was authorizing the NSA's domestic collection of data and communications about foreign targets without the requirement of an individual order based on probable cause—a requirement that seems inappropriate as applied to foreign targets outside the United States who, as discussed below, lack the protection of the Fourth Amendment. In this view, section 702 is the twenty-first century analogue to the NSA's collection of long-haul satellite communications from listening stations inside the United States. In other words, section 702 provides that the NSA may collect international communications inside the United States not only from the air—as it could in Frank Church's day—but also from a wire, so long as the intentional targets of the NSA's collection are not US persons.

If we are mostly concerned that the NSA's capabilities should not "be turned around on the American people," as Church was, the most important questions are (1) how do we ensure the NSA's targets are, in fact, foreign citizens outside the United States, and (2) how do we protect the privacy of US person information—communications to, from, or about US persons—that are collected along with the communications of foreign targets? The legal framework devised by Congress in 1978 for signals in the air and communications collected overseas left these questions to the executive branch. By contrast, section 702 requires that the NSA adopt procedures to address these concerns and submit them for approval to the Foreign Intelligence Surveillance Court. If the court determines they are adequate, and the other requirements of section 702 are met, it issues an order compelling a communications service provider to assist the NSA in collecting the information.

The requirement of prior judicial review for these procedures prompts a few significant questions. If section 702 is the digital age equivalent of the NSA's signals intelligence activities, why is the Foreign Intelligence Surveillance Court involved at all? Instead of creating a new form of FISA court order, why didn't Congress simply rewrite the outdated definition of electronic surveillance in FISA § 101(f), exempting such collection from FISA altogether? If the NSA can be trusted to handle privacy issues appropriately when it collects communications overseas or from satellites, why subject to judicial review its collection of communications from servers and switches inside the United States—so long as the NSA does not intentionally target a US person?

One response is that the court's involvement is needed because communications service providers want the protection of a court order so they can cooperate with the NSA without fear of being sued. This answer is unsatisfying, as 18 U.S.C. § 2511(2)(ii) already provides a process by which the attorney general may certify to a telecommunications provider that its assistance in collecting foreign intelligence is lawful, providing legal immunity

for the company. There is no reason that a similar process could not be used to immunize communications service providers for assisting the NSA in collection of the kind now authorized by the Foreign Intelligence Surveillance Court under section 702 even in the absence of a court order.

In fact, Congress opened the door to this approach in section 702's short-lived predecessor, the Protect America Act of 2007. Section 2 of that law contained a proviso that made review by the FISA court of programs like the ones now authorized by section 702 optional: "Nothing in the definition of electronic surveillance under section 101(f) shall be construed to encompass surveillance directed at a person reasonably believed to be located outside of the United States." As communications providers insisted on court orders, the language had little practical impact. Still, as the Bush administration sought support in Congress for a replacement for the Protect America Act, there was strong opposition to retaining this language. In debate on passage of the FISA Amendments Act in March 2008, Nancy Pelosi, the Speaker of the House, explained its removal as an important victory. By refusing to "follow the Senate in excluding from the definition of electronic surveillance activities historically considered within that definition," Pelosi explained, the House was ensuring privacy protections that are "very important to each and every person in America."[11] Along with a number of other members of Congress, both Pelosi and Senator Barack Obama voted against the Protect America Act, but for the FISA Amendments Act because it included more civil liberties safeguards.

There is something about section 702 collection—providing the NSA with the ability to obtain communications without probable cause and on a broad scale—that makes us particularly nervous. Our lives involve a stream of electronic communications, leaving behind digital footprints. Some of these communications—we do not know how many—cross international boundaries, and many involve non-US persons. As a result, we do not feel as Congress did in the late 1970s, when it was considering the NSA's acquisition of international telephone calls and telegrams from satellites. In the age of the Internet, we do not trust the NSA to protect our privacy with procedures that are administered entirely within the executive branch. We would like a court to act as a check on the NSA.

If this is the reason why section 702 collection requires oversight by a court, the implications for the NSA's global surveillance operations are profound. If we do not trust the NSA to administer its own targeting and minimization procedures when it collects communications from Internet gateways or servers inside the United States, why would we trust it to do so just because those gateways and servers are overseas? Just as data belonging to foreign citizens is more likely to be found in the United States than it was in the 1970s, data belonging to Americans is now more likely to be found overseas. The ease with which data travels across jurisdictions makes an approach to protecting civil liberties that depends on the territory in which data is located inherently arbitrary and problematic.[12] Modern

Internet protocols can even be manipulated to route traffic through a favored jurisdiction, prompting speculation the NSA might consider doing so in order to take advantage of the looser rules that apply to overseas collection.[13]

In sum, technology is not the only thing that has changed since 1978. The nature of our global society has changed. The Foreign Intelligence Surveillance Act does not simply contain a few outdated, technology-specific definitions. Its basic premise is outdated. Drawing a sharp distinction between global intelligence collection programs based on where and how data are collected no longer appears to be a workable way of protecting privacy, even if we care only about the privacy of Americans.

Today, the only way to fully protect Americans' privacy is to subject the NSA's global programs of surveillance to the scrutiny of all three branches of government, which means subjecting them to FISA. One way to do this is suggested by the much-maligned section 702 of FISA. A reformed section 702 of FISA could be the model for a new provision in title VII of FISA requiring authorization of the NSA's global surveillance programs by the Foreign Intelligence Surveillance Court.

There would be one significant difference between section 702 and the new provision of FISA. Section 702 gives the Foreign Intelligence Surveillance Court the authority to issue orders compelling the assistance of American companies. Such companies are within the jurisdiction of the federal courts and are subject to American law. Overseas companies are not. A new FISA provision would merely give authority to the intelligence community to collect signals intelligence, whether directly or through foreign partners. Companies that cooperate with the NSA could be made immune from liability in American courts under 18 U.S.C. § 2511(2)(ii).

A new FISA provision for signals intelligence collection would be conceptually radical, but it would actually prove modest in its practical implications for NSA operators and analysts. The provision could be as simple as a yearly application to the Foreign Intelligence Surveillance Court for authorization to collect foreign signals intelligence. Exceptions might be made for tactical military signals intelligence or for other forms of NSA collection that do not appear to raise substantial privacy issues, such as collection that is narrowly targeted to a specific network that is reserved for the communications of a foreign government.

The government's application would include three main elements: foreign intelligence, protection of US persons, and broader privacy interests.

- *Foreign intelligence*. The application would include a declaration that the purpose of the program is to collect foreign intelligence (using the narrower definition provided by FISA § 101(e), 50 U.S.C. § 1801(e), in place of the almost boundless definition in E.O. 12,333, discussed below). It would be accompanied by a copy of the National

Intelligence Priorities Framework and a description of how the intelligence community will use signals intelligence collection to satisfy the requirements of that framework.

- *US persons*. As it does for section 702 of FISA, the government would submit the targeting procedures the intelligence community intends to use to ensure its collection targets non-US persons located outside the United States and the minimization procedures used to protect information to, from, or about US persons. These would be based on United States Signals Intelligence Directive 18, the NSA's implementing rules for E.O. 12,333.[14]

- *Broader privacy interests*. The government would detail its procedures for protecting the privacy of foreign persons, as described in Presidential Policy Directive 28 (PPD-28), including its process for determining when to collect signals intelligence in bulk under that directive. The government should also describe its process for deciding when to exploit communications insecurities to collect foreign intelligence (i.e., the vulnerabilities equities process).[15]

The court would review the application and the procedures to determine if they adequately protect constitutional rights. Although United States v. Verdugo-Urquidez holds that the Fourth Amendment does not apply to searches of foreign persons outside US territory, that does not mean the exercise is pointless.[16] That case involved a physical search, not collection of communications. When the NSA targets a foreign person, it incidentally acquires the communications of the US persons inside the United States with whom that target is in contact—communications that are protected by the Fourth Amendment. The court's review would address whether the protections provided by all of the NSA's procedures, taken as a whole, satisfy the reasonableness requirements of the Fourth Amendment.

While the US person procedures are most directly relevant to the Fourth Amendment inquiry, all of the procedures matter given the increased incidental collection of US person information in the Internet age. The National Intelligence Priorities Framework ensures that NSA analysts do not have unfettered discretion in selecting communications for monitoring. The guidance provided by PPD-28 for protecting the privacy of foreign persons is helpful in protecting the privacy of US persons by offering a framework that restrains NSA activities generally. Likewise, the NSA's process for determining when to exploit vulnerabilities in commercial information technology may have a substantial impact on the privacy of US persons.

While the court's review could be limited as a formal matter to the protection of constitutional rights, the process would still provide protection for foreign persons. If the court determines that the application and the procedures are adequate, either as submitted or as modified based on the court's review, it would issue an order authorizing the NSA to collect signals intelligence subject to those procedures. Because the procedures would be

incorporated into the court's order, violations would have to be reported to the court, which would have the authority to inquire further and order remedial action. The NSA's rules would no longer be the exclusive province of the executive branch.

Little would change on the first day the NSA's overseas signals intelligence operations became subject to FISA. The NSA already adheres to all the above procedures. The Foreign Intelligence Surveillance Court's review of section 702 shows that it is likely the government's application would be approved. The court has demonstrated its willingness to accommodate the government's national security needs and to work with the agency to address problems. Its experience in overseeing programs authorized by section 702, along with its experience with NSA bulk collection programs involving telephone and Internet metadata, shows that the court is capable of playing a constructive role.

Over time, the NSA will find, as it did with those programs, that there is a big difference between observing one's own guidelines, however faithfully, and complying with court-ordered rules whose violation raises the specter of judicial sanctions. The NSA has reported a handful of incidents in which analysts used overseas collection to spy on ex-girlfriends.[17] If overseas programs were authorized by a court, an NSA analyst who intentionally misused agency resources in this way would face not only internal sanctions, but criminal liability under FISA. As the court gains experience, it could tighten procedures that have proved too weak to prevent recurring violations, or sanction more flexibility in procedures that have become outdated or unworkable. The court's opinions will also facilitate oversight by Congress and, to the extent its opinions are released in unclassified form, by the public.

Congressional authorization and meaningful court review would also put US surveillance programs and those of its closest partners on a stronger footing against human rights challenges. The European Court of Human Rights is considering three cases against the United Kingdom involving mass surveillance.[18] In these cases, a highly respected international court whose decisions are binding on the United Kingdom will consider whether the surveillance practices of its signals intelligence agency, the Government Communications Headquarters (GCHQ), interfere with the right to privacy protected by the European Convention on Human Rights. The United Kingdom is the oldest and among the closest of US allies in signals intelligence—a partnership that grew out of World War II and the Cold War.

To determine whether the GCHQ's programs and its cooperation with the NSA are lawful, the European Court of Human Rights will apply its precedents concerning surveillance by intelligence agencies. Under the convention, surveillance must be "necessary" and "proportionate" in a democratic society and it must be "in accordance with law." To satisfy these requirements, the European Court of Human Rights demands a law passed by a legislature and review by an independent body, such as a court. It will be an uphill battle to convince the court to uphold the bulk collection of signals intelligence by GCHQ and

NSA under precedents that appear to require individualized suspicion for surveillance.[19] It would be easier to do so if both GCHQ's and NSA's programs were authorized by statute and subject to meaningful judicial oversight.

While the United States is not subject to the European Convention on Human Rights, it is a party to the International Covenant on Civil and Political Rights and other international instruments that guarantee a similar right to privacy. The United States takes the unpopular and controversial position that its human rights obligations do not apply to conduct outside its own territory.[20] While the United States is likely to continue to adhere to this position as a formal matter, subjecting the NSA's overseas signals intelligence collection to judicial review offers a more palatable basis for defending global surveillance practices.

An even stronger case could be made for NSA surveillance if the Foreign Intelligence Surveillance Court's review of NSA procedures were to incorporate human rights standards of proportionality and necessity, in addition to the Fourth Amendment's requirements of reasonableness. Providing expanded rights for foreign citizens may be politically infeasible. Still, even if court review is limited to the Fourth Amendment, an expanded judicial role will still add rigor to the intelligence oversight system. Such rigor would provide meaningful, if indirect, benefits for foreign privacy. However the European Court of Human Rights rules in the UK cases, the United States could persuasively argue in international human rights forums that it has taken strong steps—stronger than those of virtually any nation—to subject its external surveillance practices to the rule of law.

Step 2: For democratic nations that agree to reform surveillance on a reciprocal basis, limit surveillance to international terrorism and other specific security threats.

The NSA's collection inside the United States of data and communications that belong to foreign persons is not very popular abroad, even among other democratic nations. While such collection is subject to judicial review under section 702 of FISA, this has done little to reassure the global public. One reason is that the judicial review provided by section 702 of the NSA's targeting and minimization procedures is designed only to protect the privacy of Americans. The NSA has used section 702 of FISA to collect data from a very large number of foreign targets. In 2015, the Foreign Intelligence Surveillance Court approved a single order under section 702 authorizing surveillance of 94,368 foreign persons whose data and communications found their way into the United States. In the same year, traditional FISA orders against foreign powers and foreign agents affected only 1,585 targets.[21]

Section 702 was primarily justified as way of monitoring international terrorists. However, the law goes far beyond this, giving the NSA broad discretion to obtain "foreign intelligence"—a term that FISA defines to include any information relevant to US foreign affairs and national defense.[22] In 2014, the Pew Research Center asked almost 50,000 people

in forty-four countries what they thought of US government surveillance. Unsurprisingly, the global public strongly opposed US surveillance of their own countries' citizens and leaders; 81 percent found US monitoring of their countries' citizens unacceptable, while 73 percent objected to monitoring their countries' leaders. The global public also objected (by a smaller margin) to US surveillance of American citizens, with 62 percent opposed. However, if US surveillance were limited to suspected terrorists, a surprising 64 percent of foreign respondents—a majority—were willing to support it.[23]

The United States works closely in the struggle against international terrorism and other serious security threats with the governments of many democratic countries. The "Five Eyes"—the United States, United Kingdom, Canada, Australia, and New Zealand—form a unique partnership in signals intelligence that requires a high level of trust. The "Five Eyes" have tacitly agreed to give up spying on each other in order to pool their surveillance resources against common global threats. International cooperation would be enhanced if a larger collection of democratic nations could agree to refrain from using their most advanced surveillance capabilities for political spying.

Judicial review offers a way to make such a promise stick. The NSA could seek authorization to target the citizens of some nations using a narrower set of criteria, if those nations agreed to do likewise and adopt meaningful surveillance reforms that would make such promises credible. A starting point could be the six national security threats that permit bulk collection of signals intelligence under Presidential Policy Directive 28 (PPD-28). They are espionage, terrorism, proliferation of weapons of mass destruction, cybersecurity threats, threats to US or allied military forces, and transnational crime.[24]

Narrowing the surveillance criteria that apply to citizens of friendly nations on a reciprocal basis could aid the US in its strained relationship with Europe when it comes to privacy. In October 2015, the Court of Justice of the European Union struck down a pillar of transatlantic commerce—the "safe harbor" agreement that allows routine transfers of personal data from the European Union to the United States. In Schrems v. Data Protection Commissioner, the Court of Justice found that NSA surveillance programs under section 702 of FISA threaten the privacy of European citizens.[25]

European law provides privacy guarantees for personal data and prohibits transfers of such data to countries outside the European Union unless those countries offer an "adequate level of protection"—which, according to the Court of Justice, means that privacy protections must be "essentially equivalent" to those of EU countries. The US-EU safe harbor scheme, administered by the US Department of Commerce, was intended to satisfy this adequacy standard. Companies agreed to follow required privacy principles by signing up to the scheme.[26] Although signing up was voluntary, the promises, once made, were enforced by the Federal Trade Commission. Against companies, these protections were more than theoretical—the FTC took many enforcement actions under the safe harbor scheme.[27]

The Snowden revelations that began in 2013 highlighted a weakness in the safe harbor agreement. Safe harbor did nothing to restrict US government surveillance. Instead, the agreement provided that companies must obey US law, even if doing so would otherwise violate the privacy commitments those companies had made. So, while an EU citizen like Max Schrems might challenge how Facebook was handling his data under the safe harbor principles, if Facebook gave his data to the NSA under section 702, he had no meaningful recourse. The European Court of Justice decided this failure doomed the safe harbor agreement.

American officials find the Schrems debate maddening, for at least two reasons. First, the personal data of EU citizens enjoys more, not less, legal protection under US law if the data is inside the United States than if it is outside the United States. Under existing law, Max Schrems's Facebook data has more protections under US law if it is on a server in America than if it is in Europe. After the Snowden revelations began in 2013, privacy-minded companies and individuals have begun to concern themselves with the location of their personal data. Those who distrust the United States for its surveillance practices may seek to ensure that data stays offshore. The problem is that offshoring data won't protect it from the NSA, and neither will keeping personal data in Europe.[28] Under E.O. 12,333, the NSA has broad authority to collect data overseas, subject to fewer protections than data collected inside the United States under FISA. This concern would be largely resolved by amending FISA so that it covers all major NSA collection programs.

Second, the NSA faces more legal scrutiny under US law to obtain Max Schrems's Facebook data in the United States than do most intelligence services in the world. The laws of many European countries do not require judicial review for intelligence surveillance. Few countries employ the safeguards the United States requires for surveillance for intelligence purposes, even against their own citizens. Of four European countries included in the Center for Democracy and Technology's comparative analysis of surveillance laws, only Italy requires a court order for intelligence surveillance. France, Germany, and the United Kingdom do not.[29] The standards for surveillance applied by other democratic countries have long been more permissive than those that apply to the US intelligence community. After the terrorist attacks in Paris and Brussels, they have been getting worse, not better.[30]

If the fact that a country provides broad legal authority for national security surveillance means that the European Union does not consider it a safe jurisdiction for storing data about its citizens, it will need to examine the laws of its own member states. The European Union will also need to look at the laws of many other countries concerning national security surveillance, starting with those it has determined provide an "adequate level of protection" for personal data. Israel is on that list. Unsurprisingly, Israel does not require a court order for national security surveillance. US officials have reason to complain that the European Union is holding US surveillance practices to an unfairly high standard.

It is important to note that the European judges in Schrems did not actually examine US surveillance programs, but instead relied on a European Commission report that was flawed in its analysis of US law.[31] The Court of Justice's main problem with section 702 is that it believed the law allowed "access on a generalised basis to the content of electronic communications." In other words, the Court of Justice regarded section 702 of FISA as mass surveillance. The court said such surveillance "must be regarded as compromising the essence of the fundamental right to respect for private life."[32]

While the mass surveillance description is accurate as applied to some NSA programs under E.O. 12,333, it is debatable as applied to section 702 of FISA. Peter Swire—a member of President Obama's independent review group, established after the Snowden revelations to review NSA programs—objects strongly to the idea that section 702 can be seen as "mass surveillance." As Swire points out, section 702 requires that NSA identify specific targets through the use of strong selectors, such as a telephone number or e-mail address.[33] The European Commission report seems to have conflated Prism—a program based on section 702 of FISA that permits surveillance of (an admittedly very large number of) specific targets—with bulk collection. The NSA's bulk collection programs involved metadata, not content, and were based on entirely different provisions of FISA. The NSA's bulk collection of telephone metadata ended in 2015 when Congress passed the USA FREEDOM Act.

The European Commission also refused to take account of surveillance reforms implemented since 2013, such as PPD-28. Cameron Kerry, a former acting Secretary of Commerce in the Obama administration, notes the robust oversight mechanisms that apply to the US intelligence community.[34] All these points are valid, and go some way toward satisfying the European Court of Justice's concerns about proportionality and "appropriate and verifiable safeguards."[35] Still, Schrems lays out standards for intelligence surveillance that US law currently does not meet. While section 702 may not authorize bulk collection because it requires selectors that are associated with particular targets, it offers little substantive protection to non-US persons.

Under section 702, the NSA may select as a target any foreign person outside the United States if it believes it may obtain "foreign intelligence information," a very broad standard. Again, the flawed premise of Schrems—that data can be protected by keeping it away from the United States—is not without considerable irony. The standard that the intelligence community uses to obtain data inside the United States under FISA is narrower than the standard it uses to obtain data outside the United States. While FISA's definition of foreign intelligence is broad, E.O. 12,333's definition of foreign intelligence is almost boundless, at least if read literally. It includes any information about the "capabilities, intentions, or activities" of foreign governments, organizations, terrorists—and even ordinary "foreign persons."[36] If Max Schrems succeeds in keeping his data outside the United States, it

-1__
0__
+1__

may or may not be more difficult for the NSA to obtain it as a practical matter. That will depend on the NSA's ability to access it, which in turn depends on its partnerships and its operational effectiveness. It will be trivial to do so as a legal matter. Since Max Schrems is a foreign person, his "capabilities, intentions, or activities" are by definition foreign intelligence. If FISA is amended to encompass the NSA's foreign programs, the anomaly goes away because the narrower definition of foreign intelligence information would apply in either case.

Nevertheless, even the narrower definition does not satisfy the standards that the European Court of Justice provided for intelligence surveillance in Schrems. The court explained that intelligence surveillance can only be justified by reference to an "objective criterion" that limits surveillance to "purposes which are specific, strictly restricted, and capable of justifying the interference which both access to that data and its use entail."[37] A broad authorization to obtain "foreign intelligence information," like the one contained in section 702 of FISA, simply does not meet this standard. A narrower set of criteria related to specific security threats, like those provided in PPD-28, is much easier to justify. Combatting espionage, terrorism, proliferation of weapons of mass destruction, cybersecurity threats, threats to US or allied military forces, and transnational crime are all certainly "legitimate objectives," that are "based on considerations of national security or the prevention of crime."[38]

Adopting these criteria for NSA surveillance of EU citizens would require that all sides give something up. Privacy advocates would have to accept an agreement for data transfer that would continue to allow the NSA to access European data, under a narrower set of criteria. The US intelligence community would sacrifice foreign affairs surveillance involving citizens of EU members, along with other democratic nations if they agree to similar limits. European intelligence services would have to take reciprocal steps.

The high standards to which the Court of Justice subjected government surveillance in Schrems offer a unique opportunity for global surveillance reform. If EU institutions are serious about subjecting surveillance laws to real scrutiny, those standards could build momentum for reform of those laws—and not just in the United States and Europe. Schrems laid down rules for intelligence surveillance that all countries must meet to do business with Europe, if they expect to engage in seamless transfers of personal data.

Countries that ignore human rights decisions may be subject to international embarrassment and criticism, but they rarely suffer more tangible consequences. The Court of Justice of the European Union, however, is not a human rights tribunal—it is the supreme judicial authority of a unique supranational organization. The court serves as a guardian for the rules that govern the European Union's common market in goods and services. The US-EU relationship is vital to global trade, and not just for big technology firms like

Facebook and Google. Safe harbor involved more than 4,000 companies.[39] In the age of big data, it is unthinkable that international companies can do business without routine transfers of personal data. The global economy depends on hammering out agreements that allow those transfers to take place—and that will stand up in European courts.

In February 2016, the United States and the European Union announced an agreement to replace safe harbor: the Privacy Shield. It falls far short of the reforms advocated in this paper. The agreement offers a nod to concerns about government surveillance by requiring a US official to hear European complaints against the intelligence community. Also as part of the agreement, the chief lawyer for the US intelligence community provided a detailed description of US limits on surveillance, including reforms implemented since 2013.[40] Apparently, the hope is that Schrems can be addressed with a few cosmetic changes to the safe harbor framework and by explaining that the European Commission got its analysis of section 702 of FISA wrong.

In my view, this hope is in vain.[41] The Privacy Shield will certainly be challenged in court, and such a challenge is likely to succeed. Striking a deal with EU bureaucrats is not going to do the job in the long run without surveillance reform. The decisions of the Court of Justice on European law are final and binding, and its decisions on privacy and data protection are intertwined with fundamental human rights principles which do not afford much wiggle room.

Narrowing surveillance criteria under either section 702 of FISA or a new provision governing other NSA programs might be seen as naïve. Should we really trust other governments, even democratic ones, to tie their own hands? There is no need for blind trust. The United States should require that nations who want narrower criteria for surveillance of their citizens by the NSA adopt meaningful surveillance reforms, such as review of surveillance programs by an independent judiciary. Of course, there are costs if the United States chooses to give up the use of NSA signals intelligence for general "foreign affairs" surveillance, even if only for other democratic nations that agree to limit their own surveillance programs. "Foreign affairs" surveillance provides real value, especially as it may aid in combatting international corruption, enforcing economic sanctions, and policing trade agreements.[42]

Other democratic governments engage in broad "foreign affairs" collection. The Snowden revelations unleashed an avalanche of hypocrisy from many governments protesting intelligence surveillance of the sort that they routinely practice. If "hypocrisy is the tribute that vice pays to virtue," as François de la Rochefoucauld once said, in the past few years foreign government criticism has done much to pay homage to the NSA.[43] As surveillance faces increased scrutiny from international courts and institutions, hypocrisy on surveillance no longer appears to be a sustainable strategy. Henry Farrell and Martha Finnemore note that a major effect of the Snowden leaks has been to "undermine

Washington's ability to act hypocritically and get away with it."[44] One could make the same point about many other democratic governments.

Despite the failure of many governments to live up to values of privacy, human rights, and data protection, these values are plainly a force for good in the world. America shares these fundamental values. It would support these values if it could agree with other democratic nations to cut back on the collection and use of private data and communications except in cases of genuine security threats.

Step 3: Allow court challenges to NSA surveillance, even where challengers cannot prove their communications were intercepted.

If the US government wants to maintain credibly that the NSA is accountable to the rule of law, it must provide effective redress for unlawful surveillance. The Privacy Act provides access and correction rights for data held by government agencies, but the government's legitimate need for secrecy makes it a poor tool for challenging surveillance practices. The existing civil action for unlawful surveillance suffers from the same problem—how would anyone know to invoke it? The most important reform that Congress could make to provide effective redress is explicitly to allow people who reasonably fear NSA surveillance to challenge it in court, in the expectation that a new Supreme Court may reconsider its decision barring such challenges in light of changed circumstances since 2013.

In Schrems, the European Court of Justice said that the "fundamental right to effective judicial protection" requires that a person have "legal remedies in order to have access to personal data relating to him" and the ability "to obtain the rectification or erasure of such data."[45] The court also found that US law does not provide meaningful redress for EU citizens whose data is collected by the NSA. For years, European officials have been asking for the United States to make available to citizens of the European Union some form of redress for privacy harms. During the Bush years, the Department of Homeland Security put in place a privacy-friendly departmental policy extending Privacy Act rights to non-US persons.[46] In 2013, the President's Review Group—established in the wake of the Snowden revelations—recommended that Congress amend the Privacy Act to provide rights for foreign citizens. In February 2016, Congress responded with the Judicial Redress Act. The new law provides limited Privacy Act rights to citizens of countries designated by the attorney general, with the concurrence of the secretaries of state, treasury, and homeland security. It has the support of technology companies, privacy organizations, and the Obama administration.[47]

Nevertheless, the Privacy Act does not provide anyone, US person or otherwise, meaningful redress for NSA surveillance. Agencies can exempt themselves from the Privacy Act's access and redress provisions on grounds of national security, and the NSA has taken full advantage of this section.[48] The broader reforms to the Privacy Act urged by privacy groups

would do nothing to change this. Indeed, in its letter on the Judicial Redress Act, the Electronic Privacy Information Center relied on these exemptions to explain why extending broader Privacy Act rights to non-US citizens would have no effect on national security.[49] Of course, the exemptions are there for a reason. To state the obvious, if the NSA obtains data belonging to a terrorist who is in Paris and may be planning an attack, it should not have to provide the target with access to his files and the ability to correct them. The Bill of Rights is not a suicide pact, and neither is the Privacy Act. While the targets of NSA surveillance include more than terrorists—and would continue to do so even under a narrower set of criteria—it makes no sense to undermine legitimate surveillance by granting targets access to their files.

Cameron Kerry and Alan Raul—a former member of a privacy board during the George W. Bush administration—argue that there is already redress for victims of unlawful surveillance under section 702 of FISA. They point out that foreign citizens may sue for civil damages under 50 U.S.C. § 1810 if they can show they have been subject to unlawful surveillance. The problem, of course, is: How can anyone show she is a victim of surveillance that is secret?[50] Neither the Privacy Act nor the existing private action for unlawful surveillance offers meaningful judicial redress. The NSA's targets are secret—and we would like to keep it that way.

A better approach to the issue of redress would be to allow those with reasonable fears of surveillance to challenge the NSA and other intelligence agencies in court, without the need for the government to confirm or deny that their communications are being intercepted. Human rights law has long allowed such challenges. In the 1978 case of Klass v. Germany, the European Court of Human Rights addressed whether people who challenge surveillance programs can claim to be "victims of a violation" of the European Convention on Human Rights if they do not know whether they are under surveillance. The court decided that they could, reasoning that it was "unacceptable" in a democratic society for surveillance to remain "unchallengeable" because of its secrecy.[51]

The problem is that American law takes the opposite view. In Clapper v. Amnesty International, decided in early 2013, the Supreme Court ruled against a challenge of section 702 of FISA because the plaintiffs could not show that their communications had been intercepted under that law.[52] Writing for the majority, Justice Samuel Alito wrote that the plaintiffs had not alleged the sort of concrete injury needed for their complaints to qualify as one of the proper "Cases" or "Controversies" that Article III of the US constitution permits the judicial branch to hear.

The plaintiffs in Clapper were not wearers of tinfoil hats. Instead, they were international human rights lawyers, reporters, and researchers whose communications put them in touch with the sort of people—including associates of terrorist organizations—who were likely enough to be NSA targets. Nevertheless, the plaintiffs' reasonable fears of surveillance

were not enough to have their complaints heard on the merits. Instead, they had to show that surveillance of their communications was "certainly impending" in order to establish "Article III standing" to sue.

Clapper was decided on constitutional grounds. If Congress amended FISA to allow foreign citizens to challenge NSA surveillance programs, plaintiffs would still have to meet Article III standing requirements. The Supreme Court regards standing requirements as an aspect of the separation of powers. They limit Congress's ability to create "citizen suits" in environmental matters—and, *a fortiori*, its power to create "foreign citizen suits" to address fears of mass surveillance.[53] The Article III law of standing is not just a problem for responding to the human rights concerns of foreign citizens about privacy—it is also the single biggest obstacle for Americans' ability to hold their own intelligence agencies to account in court for their surveillance practices.

While Clapper seems to foreclose most challenges to NSA surveillance, its reasoning makes less sense in a post-Snowden world. In Clapper, Justice Alito pointed to a "highly attenuated chain of possibilities" to describe why the plaintiffs could not show concrete injury from section 702 of FISA. To show standing, plaintiffs had to assume that:

1. the Government will decide to target the communications of non-U.S. persons with whom they communicate;

2. in doing so, the Government will choose to invoke its authority under [FISA section 702] rather than utilizing another method of surveillance;

3. the Article III judges who serve on the Foreign Intelligence Surveillance Court will conclude that the Government's proposed surveillance procedures satisfy [section 702]'s many safeguards and are consistent with the Fourth Amendment;

4. the Government will succeed in intercepting the communications of respondents' contacts; and

5. respondents will be parties to the particular communications that the Government intercepts.[54]

Clapper was decided in early 2013, when Edward Snowden was still an anonymous NSA contractor living in Hawaii. The Snowden revelations and the intelligence community's own transparency drive have undermined much of what the Supreme Court said to reject standing in that case. Today, the chain of possibilities described by Justice Alito has become much less speculative, especially if—as recommended above—Congress extends judicial review under FISA to all major NSA surveillance programs and creates a remedy for unlawful surveillance that applies to foreigners.

- First, a foreign citizen may actually have an easier time establishing standing than the American plaintiffs did in Clapper. Foreigners' communications can be targeted directly under section 702 of FISA, making their fears of surveillance less speculative.

- Second, the government has confirmed that it has obtained orders for surveillance of foreign citizens under section 702 and has declassified details of two NSA programs—Prism and upstream collection.[55] These descriptions make clear that the NSA's interception has been successful and the programs have collected a very broad set of communications.

- Third, the plaintiffs in Clapper, the Supreme Court observed, "have no actual knowledge of the government's [section 702] targeting practices." As a result of the intelligence community's post-Snowden transparency drive, now they have considerable detail about these practices.[56]

- Finally, if FISA were extended to cover all major forms of NSA surveillance, a foreign plaintiff would have little or no trouble showing it is reasonable to assume that surveillance can be traced either to section 702 or to another, very similar provision in title VII of FISA for overseas surveillance, as opposed to some other legal authority with different standards of proof. Under such a legal framework, title VII of FISA would occupy the field of NSA surveillance directed at foreign citizens outside the United States.

With these facts in mind, consider a prominent foreign scientist working on nuclear issues involving Iran who communicates with other scientists and government officials around the world. Given all that the government has confirmed about the NSA's activities, it is far more difficult to describe such a scientist's fears of NSA surveillance as "attenuated." Ironically, an American nuclear scientist would have a much harder time.

Clapper poses one final obstacle in any challenge the scientist might bring: she does not know whether her e-mail address is actually on the NSA's target list. Because doubt remains about whether the scientist is actually under surveillance, it may not be literally true to say that surveillance is "certainly impending." Developments since Clapper provide a strong argument for reconsidering such a rigid approach. These developments vividly demonstrate how an overly cramped view of Article III standing shields intelligence agencies from having to defend surveillance practices on the merits.

In Clapper, the Supreme Court accepted a government argument that has since been discredited. At oral argument, Solicitor General Donald Verrilli said that a failure to find standing would not insulate surveillance under section 702 of FISA from judicial review. The government would be required to disclose such surveillance in any future criminal prosecution, Verrilli assured the justices, and a defendant would then be able to challenge

evidence that had been derived from it. While the argument was not decisive, it was embraced in Justice Alito's opinion. After Clapper was decided, Verrilli was embarrassed to learn that the Justice Department had not, in fact, been disclosing its use of section 702 surveillance to obtain evidence in criminal cases. Clearly, after-the-fact judicial review of intelligence surveillance is not as straightforward as the Supreme Court believed it to be. This episode bolsters the argument for a more flexible approach to standing than a strict reading of the "certainly impending" injury requirement might permit, in order to preserve the very Article III values that the standing doctrine embodies.[57]

In 2016, the Supreme Court returned to the question of standing in another case in which Justice Alito wrote the Court's opinion. Spokeo v. Robins concerned whether a person whose records were mishandled by an Internet search engine has standing to sue if the only harm he alleges is a violation of his statutory rights under the Fair Credit Reporting Act. Justice Alito noted that Congress cannot "erase Article III's standing requirements by statutorily granting the right to sue to a plaintiff who would not otherwise have standing." A purely legal harm was not enough, he said; the harm must be " 'de facto'; that is, it must actually exist." "This does not mean, however, that the risk of real harm cannot satisfy the requirement of concreteness," Alito wrote, or that harm must be tangible. Spokeo returned the case to the lower courts to decide if the plaintiff had met these requirements.[58]

Intriguingly, Alito cited Clapper in support of his point that the mere "risk of real harm" may be enough for standing. The surprising way in which Alito cited Clapper sheds new light on his opinion in that case. In Clapper, Alito had used a footnote to suggest the possibility of a more flexible approach to standing in a future case than the requirement of "certainly impending" injury would suggest. "Our cases do not uniformly require plaintiffs to demonstrate that it is literally certain that the harms they identify will come about. In some instances, we have found standing based on a 'substantial risk' that the harm will occur, which may prompt plaintiffs to reasonably incur costs to mitigate or avoid that harm."[59] Alito gave no indication in Spokeo that the court might reconsider its view that plaintiffs like those in Clapper lack standing. Still, a case in which the plaintiffs' fears of surveillance were less speculative could well come out differently.

Standing would not be the only obstacle to a foreign citizen who wants to make a viable claim that NSA surveillance is unlawful. Winning such a case on the merits could be a long shot. As discussed above, foreigners outside the United States lack Fourth Amendment rights, and the government argues that human rights treaties do not apply to its conduct abroad. Unless Congress made clear that foreign citizens could challenge NSA surveillance under some theory, it is hard to see how our scientist could state any viable claim. Of course, in a sense, that is the point. NSA surveillance under a reformed FISA would include new safeguards, designed to meet constitutional standards of Fourth Amendment reasonableness. The reforms outlined above, including judicial review of overseas NSA surveillance and narrower criteria for some foreign citizens, would arguably meet human

rights standards—"in accordance with law," "necessity" and "proportionality"—as well. Because the government should have confidence that its surveillance will withstand judicial scrutiny on the merits, it should not have to hide behind an artificial and technical defense like standing.

Conclusion: The Global Logic of Surveillance Reform

During the Obama years, the United States took bigger steps in the direction of reforming surveillance than many appreciate.[60] There has been increased transparency from the US intelligence community, and now the Office of the Director of National Intelligence has provided a mechanism for institutionalizing it.[61] Presidential Policy Directive 28 (PPD-28) provides limited privacy protections for non-US citizens located abroad. Congress has ended bulk collection of telephone metadata from American companies. These reforms do not have the same global implications as the comprehensive NSA reforms advocated in this paper. Increased transparency and privacy protections for foreigners set a good example, but at bottom these are still policy changes that other countries are free to ignore.

When demonstrators from Berlin to San Francisco carry signs saying, "Thank you, Edward Snowden," there is no question that people around the world see the NSA as one of the world's chief threats to privacy. The truth about the NSA's mass surveillance operations has exceeded the most alarming visions conjured up by privacy and civil liberties activists. The other truth about the NSA, however, is just how seriously it takes the rules that govern it. The problem is that these rules, designed in the 1970s to prevent "spying on Americans," are inadequate for the digital age.

It is not just the technology-specific definitions of FISA that are out of date. The broader premise of FISA no longer holds. Carving out a subset of intelligence surveillance that affects Americans and subjecting only that subset to court oversight—while leaving the rest of the NSA's global signals intelligence operations to oversight only within the executive branch—simply does not provide sufficient privacy protection, even if the only objective is to protect the privacy of Americans.

It turns out that we are all in this together. There is no escaping the global logic of surveillance reform. If we want to protect our own privacy, we have to protect everyone's privacy. Extending FISA to cover all major NSA surveillance programs is the most promising way of doing so. The next president—and the next Congress—should go big, and go global, on reforming mass surveillance.

NOTES

1 Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (USA PATRIOT Act) of 2001, Title II, 115 Stat. 272.

2 See Privacy and Civil Liberties Oversight Board, *Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act*, July 2, 2014, 104–110, https://www.pclob.gov/library/702-Report.pdf.

3 The Senate Judiciary Committee held a hearing on May 10, 2016, that aired many of these concerns. See *Oversight and Reauthorization of the FISA Amendments Act: The Balance between National Security, Privacy and Civil Liberties*, member and witness statements, http://www.judiciary.senate.gov/meetings/oversight-and-reauthorization-of-the-fisa-amendments-act-the-balance-between-national-security-privacy-and-civil-liberties.

4 See Amos Toh, Faiza Patel, and Elizabeth Goitein, Brennan Center for Justice, *Overseas Surveillance in an Interconnected World,* March 16, 2016, https://www.brennancenter.org/publication/overseas-surveillance-interconnected-world.

5 *Presidential Policy Directive—Signals Intelligence Activities/PPD-28,* January 17, 2014, https://www.whitehouse.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities.

6 See *Supplementary Detailed Staff Reports on Intelligence Activities and the Rights of Americans,* 271–372 (warrantless FBI electronic surveillance and microphone surveillance) and 733–84 (NSA programs affecting Americans, including SHAMROCK and MINARET), in 3 FINAL REPORT OF THE SENATE SELECT COMMITTEE TO STUDY GOVERNMENTAL OPERATIONS WITH RESPECT TO INTELLIGENCE ACTIVITIES (CHURCH COMMITTEE), S. REP. NO. 94-755 (1976), http://www.intelligence.senate.gov/resources/intelligence-related-commissions.

7 Church's comments were made in an August 17, 1975, interview on NBC's *Meet the Press*. They were replayed for a roundtable discussion about surveillance on that show after the Snowden revelations began. See *MTP roundtable: Looking for patterns in an era of "Big Data,"* August 4, 2013, http://www.nbcnews.com/video/meet-the-press/52669293#52669293.

8 Glenn Greenwald, NO PLACE TO HIDE: EDWARD SNOWDEN, THE NSA, AND THE U.S. SURVEILLANCE STATE (New York: Metropolitan Books, 2014).

9 FISA § 101(f), 50 U.S.C. § 1801(f).

10 For an excellent discussion of this, see Charlie Savage, POWER WARS: INSIDE OBAMA'S POST-9/11 PRESIDENCY (New York: Little, Brown, 2015), 170–77.

11 *Debate on the FISA Amendments Act of 2008*, 154 CONG. REC. H1748 (daily edition, March 14, 2008), statement of Representative Nancy Pelosi.

12 For a good discussion of this issue, see Jennifer C. Daskal, *The Un-Territoriality of Data*, 125 YALE L. J. 326 (2015).

13 See Axel Arnbak and Sharon Goldberg, *Loopholes for Circumventing the Constitution: Unrestrained Bulk Surveillance on Americans by Collecting Network Traffic Abroad*, 21 MICH. TELECOMM. & TECH. L. REV. 317 (2015).

14 United States Signals Intelligence Directive USSID SP0018, "Legal Compliance and U.S. Persons Minimization Procedures," January 25, 2011 (declassified November 13, 2013), http://icontherecord.tumblr.com/post/67419963949/dni-clapper-declassifies-additional-intelligence.

15 The government released a declassified version of this policy in response to a request by the Electronic Frontier Foundation under the Freedom of Information Act. See "Vulnerabilities Equities Process—January 2016," https://www.eff.org/document/vulnerabilities-equities-process-january-2016.

16 United States v. Verdugo-Urquidez, 494 U.S. 259, 267 (1990) (Fourth Amendment does not apply to "aliens in foreign territory or in international waters.")

17 See Letter to Senator Charles E. Grassley from Dr. George Ellard, NSA inspector general, September 11, 2013, http://icontherecord.tumblr.com/post/62457835497/nsa-inspector-generals-letter-to-senator-charles.

18 10 Human Rights Organizations and Others v. United Kingdom, application no. 24960/15, lodged May 20, 2015, http://hudoc.echr.coe.int/eng?i=001-159526; Bureau of Investigative Journalism and Alice Ross v. United Kingdom, application no. 62322/14, lodged September 11, 2014, http://hudoc.echr.coe.int/eng?i=001-150946; and Big Brother Watch and Others v. United Kingdom, application no. 58170/13, lodged September 4, 2013, http://hudoc.echr.coe.int/eng?i=001-140713.

19 See Carly Nyst, "European Human Rights Court Deals a Heavy Blow to the Lawfulness of Bulk Surveillance," *Just Security* (blog), December 9, 2015, https://www.justsecurity.org/28216/echr-deals-heavy-blow-lawfulness-bulk-surveillance.

20 See Charlie Savage, *U.S. Seems Unlikely to Accept That Rights Treaty Applies to Its Actions Abroad,* New York Times, March 6, 2014, http://www.nytimes.com/2014/03/07/world/us-seems-unlikely-to-accept-that-rights-treaty-applies-to-its-actions-abroad.html.

21 Office of the Director of National Intelligence, *Calendar Year 2015 Transparency Report,* May 2, 2016, https://icontherecord.tumblr.com/transparency/odni_transparencyreport_cy2015.

22 See FISA § 101(e), 50 U.S.C. § 1801(e).

23 Pew Research Center, "Global Opinions of U.S. Surveillance," July 14, 2014, http://www.pewglobal.org/2014/07/14/nsa-opinion/.

24 PPD-28 at § 2.

25 Maximillian Schrems v. Data Protection Commissioner (Court of Justice of the European Union, October 6, 2015), no. C-362/14, Judgement of the Court (Grand Chamber), http://curia.europa.eu/juris/documents.jsf?num=C-362/14.

26 For more information about safe harbor, see the government's web site at http://www.export.gov/safeharbor/eu/.

27 Jedidiah Bracy, "How Julie Brill Is Cultivating a Defense of the U.S. Privacy Framework," *Privacy Perspectives,* February 24, 2015, https://iapp.org/news/a/how-julie-brill-is-cultivating-a-defense-of-the-u-s-privacy-framework.

28 Timothy Edgar, "Offshoring Data Won't Protect It From the NSA," in TechCrunch's *Crunch Network* (blog), January 2, 2015, http://techcrunch.com/2015/01/02/offshoring-data-wont-protect-it-from-the-nsa/.

29 See the discussion of national security surveillance standards in Center for Democracy and Technology, *Comparative Study of Standards for Government Access* (2013), http://govaccess.cdt.info./.

30 Nils Muiznieks, *Europe Is Spying on You* (op-ed), New York Times, October 27, 2015, http://www.nytimes.com/2015/10/28/opinion/europe-is-spying-on-you-mass-surveillance.html.

31 *Schrems* ¶¶ 13–16, 22–25, 93–94. See also "European Commission calls on the U.S. to restore trust in EU-U.S. data flows," November 27, 2013, http://ec.europa.eu/justice/newsroom/data-protection/news/131127_en.htm.

32 *Schrems* ¶ 94.

33 Peter Swire, "Don't Strike Down the Safe Harbor Based on Inaccurate Views About U.S. Intelligence Law," *Privacy Perspectives,* October 5, 2015, https://iapp.org/news/a/dont-strike-down-the-safe-harbor-based-on-inaccurate-views-on-u-s-intelligence-law/.

34 Cameron Kerry, "Finding a Safe Harbor for Safe Harbor," *Privacy Perspectives,* October 1, 2015, https://iapp.org/news/a/finding-a-safe-harbor-for-safe-harbor/.

35 *Schrems* ¶¶ 34, 90.

36 E.O. 12,333 at § 3.5(e).

-1__
0__
+1__

37 *Schrems* ¶ 93.

38 *Schrems* ¶¶ 88, 34.

39 Mark Scott, *Data Transfer Pact Between U.S. and Europe Is Ruled Invalid*, New York Times, October 6, 2015, http://www.nytimes.com/2015/10/07/technology/european-union-us-data-collection.html.

40 See Letter from General Counsel Robert Litt, Office of the Director of National Intelligence, February 22, 2016, in "EU-U.S. Privacy Shield Full Text," 104–122, https://www.commerce.gov/privacyshield.

41 See Timothy Edgar, *Privacy's New Clothes*, SC Magazine, March 16, 2016, http://www.scmagazineuk.com/privacys-new-clothes/article/479110/.

42 See Peter Margulies, *Defining "Foreign Affairs" in Section 702 of the FISA Amendments Act: The Virtues and Deficits of Post-Snowden Dialogue on U.S. Surveillance Policy*, 72 Wash. & Lee L. Rev. 1283 (2015).

43 Alan Ehrenhalt, *Hypocrisy Has Its Virtues,* New York Times, February 6, 2001, http://www.nytimes.com/2001/02/06/opinion/hypocrisy-has-its-virtues.html.

44 Henry Farrell and Martha Finnemore, *The End of Hypocrisy: American Foreign Policy in the Age of Leaks,* Foreign Affairs, November/December, 2013, https://www.foreignaffairs.com/articles/united-states/2013-10-15/end-hypocrisy.

45 *Schrems* ¶ 95.

46 Hugo Teufel, "An Explanation of the DHS Privacy Policy Behind Review Group Recommendation no. 14," *Lawfare: Hard National Security Choices* (blog), January 8, 2014, https://www.lawfareblog.com/explanation-dhs-privacy-policy-behind-review-group-recommendation-14.

47 Judicial Redress Act of 2015, Pub. L. No. 114-126, 130 Stat. 282 (2016). See also Internet Infrastructure Coalition, "Judicial Redress Act Letter," October 2, 2015, https://www.i2coalition.com/judicial-redress-act-letter/; Jens-Henrik Jeppesen and Greg Nojeim, "The EU-US Umbrella Agreement and the Judicial Redress Act: Small Steps Forward for EU Citizens' Privacy Rights," October 5, 2015, https://cdt.org/blog/the-eu-us-umbrella-agreement-and-the-judicial-redress-act-small-steps-forward-for-eu-citizens-privacy-rights/; "EPIC Recommends Changes to Judicial Redress Act," September 16, 2015, https://epic.org/2015/09/epic-recommends-changes-to-jud.html; and Shaun Waterman, "Lawmakers back privacy rights for noncitizens," *FedScoop,* September 17, 2015, http://fedscoop.com/lawmakers-back-privacy-rights-for-noncitizens.

48 5 U.S.C. § 552a(k); 32 C.F.R. § 322.7(a).

49 "Statement of EPIC on H.R. 1428, the Judicial Redress Act of 2015," September 16, 2015, https://epic.org/foia/umbrellaagreement/EPIC-Statement-to-HJC-on-HR1428.pdf.

50 Cameron F. Kerry and Alan Charles Raul, "Safeguards and Oversight of U.S. Surveillance under Section 702," *Data Matters,* October 25, 2015, http://datamatters.sidley.com/safeguards-and-oversight-of-u-s-surveillance-under-section-702/.

51 Klass and others v. Federal Republic of Germany, European Court of Human Rights, September 6, 1978, Series A, No. 28, 2 EHRR 214, ¶¶ 30, 34–38, http://www.hrcr.org/safrica/limitations/klass_germany.html.

52 Clapper v. Amnesty International, 568 U.S. __, No. 11-1025, February 26, 2013.

53 See Cass Sunstein, *What's Standing After* Lujan? *Of Citizen Suits, "Injuries," and Article III*, 91 Mich. L. Rev. 163 (1992).

54 *Clapper,* slip op. at 11.

55 See the opinion of the Foreign Intelligence Surveillance Court discussed in Benjamin Wittes and Lauren Bateman, "The NSA Documents, Part II: The October 2011 FISC Opinion," *Lawfare* (blog), August 22, 2013, https://www.lawfareblog.com/nsa-documents-part-ii-october-2011-fisc-opinion.

56 See the extensive NSA directives declassified in 2013 and available from Wells Bennett, "In Re Directives Documents Released," *Lawfare* (blog), September 11, 2013, https://www.lawfareblog.com/re-directives-documents-released.

57 See Charlie Savage, *Door May Open for Challenge to Secret Wiretaps,* New York Times, October 16, 2013, http://www.nytimes.com/2013/10/17/us/politics/us-legal-shift-may-open-door-for-challenge-to-secret-wiretaps.html; Jameel Jaffer and Patrick C. Toomey, "The Solicitor General Should Correct the Record in *Clapper*," *Just Security* (blog), October 18, 2013, https://www.justsecurity.org/2219/solicitor-general-correct-record-clapper/.

58 Spokeo v. Robins, 578 U.S. __, No. 13-1339, at 7–10 (May 16, 2016) (internal quotation marks and citations omitted.)

59 *Clapper*, 568 U.S. __, slip op. at 15 n.5 (citations omitted).

60 Timothy H. Edgar, *The Good News About Spying,* Foreign Affairs, April 13, 2015, https://www.foreignaffairs.com/articles/united-states/2015-04-13/good-news-about-spying.

61 For the new transparency plan for intelligence agencies, see Rachel Brand, "Transparency in the Intelligence Community," *Lawfare* (blog), November 2, 2015, https://lawfareblog.com/transparency-intelligence-community.

-1__
0__
+1__

The preferred citation for this publication is:
Citation TK

About the Author

TIMOTHY H. EDGAR

Author Bio TK

Working Group on National Security, Technology, and Law

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

The group focuses on a broad range of interests, from surveillance to counterterrorism to the dramatic impact that rapid technological change—digitalization, computerization, miniaturization, and automaticity—are having on national security and national security law. Topics include cybersecurity, the rise of drones and autonomous weapons systems, and the need for—and dangers of—state surveillance. The group's output will also be published on the Lawfare blog, which covers the merits of the underlying legal and policy debates of actions taken or contemplated to protect the nation and the nation's laws and legal institutions.

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

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

-1__
0__
+1__

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

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

HOOVER INSTITUTION

117-65894_ch01_1P.indd 28 6/4/16 1:39 AM