An Overview of US Surveillance in Light of 'Schrems II'

Contents

An Overview of US Surveillance in Light of 'Schrems II'

By DLA Piper Partner Andrew Serwin, CIPP/A, CIPP/C, CIPP/E, CIPP/G, CIPP/US, CIPM, CIPT

THE IMPORTANCE OF US SURVEILLANCE LAW—'SCHREMS II'

Quis custodiet ipsos custodes?[1]

"Who guards the guards" is a critical question in any civil society, and no issue captures this concern more, at least at this point in history, than skepticism over surveillance by the United States government. The purpose of this white paper is not to argue for the validity or invalidity of any particular surveillance mechanism, but rather to provide a neutral, unclassified summary of the law and authorities in this area.

The purpose of this is twofold. First, the "Schrems II" decision focuses more attention on the surveillance activities of the U.S. government, and as companies assess the adequacy of data transfers to the U.S., they should try to understand the law of surveillance, which was an important consideration in the case. This analysis is all the more important in light of the recent FAQ document issued by the European Data Protection Board.

Second, as the U.S. and European Union consider how to address the broader policy issues of data transfers, given the critical nature of the trans-Atlantic data flow, removing confusion and having clarity about the U.S. surveillance regime can only help the process try to avoid creating a mechanism that will only later be invalidated.

An overview of surveillance in the US—understanding the executive's authority

It is hard to imagine many areas of law and policy that engender more passionate feelings than the law of foreign surveillance and national security. This is all the more true as we continue to move into a more connected world in which a significant amount of electronic communications are routed through the U.S., even when no U.S. person is involved in the communication. This technological reality—that many foreign-to-foreign communications are routed or sent to the U.S.—impacts many aspects of policy and law and none more than national security law.

Looking at how we got here helps us understand where we are, as well as where we are going. How we got here, however, is a bit of a tortured path, filled with a number of misconceptions and fragmented opinions and laws. This article will attempt to lay a foundation for future articles that explain the authority and purpose of a variety of different members of the IC, as well as specific statutory enactments and EOs that help set the framework for foreign intelligence gathering in the national security context. Without this background, it is difficult at times to understand the "who," let alone the "why" or the "what."

Deconflicting presidential power

One of the most important points to consider regarding presidential power is that the president's power is not necessarily fixed, but rather fluctuates depending on the actions of Congress. One of the critical cases to consider presidential powers is Youngstown Sheet & Tube Co. v. Sawyer, 343 U.S. 579 (1952). This case arose from the seizure by the president of the majority of the nation's steel mills during the Korean War. The most relevant portion of the opinion is the concurrence of Justice Robert Jackson that identifies three scenarios that describe the president's powers.

> *"1. When the President acts pursuant to an express or implied authorization of Congress, his authority is at its maximum, for it includes all that he possesses in his own right plus all that Congress can delegate. In these circumstances, and in these only, may he be said (for what it may be worth), to personify the federal sovereignty. If his act is held unconstitutional under these circumstances, it usually means that the Federal Government as an undivided whole lacks power. A seizure executed by the President pursuant to an Act of Congress would be supported by the strongest of presumptions and the widest latitude of judicial interpretation, and the burden of persuasion would rest heavily upon any who might attack it.*
>
> *2. When the President acts in absence of either a congressional grant or denial of authority, he can only rely upon his own independent powers, but there is a zone of twilight in which he and Congress may have concurrent authority, or in which its distribution is uncertain. Therefore, congressional inertia, indifference or quiescence may sometimes, at least as a practical matter, enable, if not invite, measures on independent presidential responsibility. In this area, any actual test of power is likely to depend on the imperatives of events and contemporary imponderables rather than on abstract theories of law.*
>
> *3. When the President takes measures incompatible with the expressed or implied will of Congress, his power is at its lowest ebb, for then he can rely only upon his own constitutional powers minus any constitutional powers of Congress over the matter. Courts can sustain exclusive Presidential control in such a case only be disabling the Congress from acting upon the subject. Presidential claim to a power at once so conclusive and preclusive must be scrutinized with caution, for what is at stake is the equilibrium established by our constitutional system.*[2]"

Thus, where the president acts pursuant to his power and congressional authorization, his powers are at their highest point. Where the president acts where Congress has been silent, his

powers are lower than the first scenario, but they are higher than where he is acting in a way that is incompatible with the express or implied will of Congress.

Given the patchwork of statutes and EOs, understanding these distinctions is critical when examining surveillance authorities.

The sources of the president's authority

One of the first issues is to recognize that the president has inherent authority to conduct surveillance in the national security arena, and warrantless wiretap has a long history in the U.S., from President Franklin Roosevelt forward. The source of this authority, as discussed below, is mainly constitutional, though Congress has enacted statutes that also provide the Executive Branch authority in this arena, but it does not result from the Foreign Intelligence Surveillance Act or later EOs, such as EO 12333.

While the Executive Branch's authority has been regulated in some ways, it is clear that the Executive Branch does have independent authority to engage in foreign intelligence activities. For example, United States v. Brown, and United States v. Butenko holds that the Executive Branch has inherent power to conduct warrantless surveillance in the foreign intelligence space.[3] As noted below, many other courts, including the Supreme Court, have noted the power of the Executive Branch to conduct surveillance, though the holdings are not as clear as these two cases.

In making the case to support certain of the activities of the National Security Agency post-9/11, the Department of Justice made its case quite directly—that the foreign intelligence activities of the NSA were supported "by the well-recognized inherent constitutional authority as Commander in Chief and sole organ for the Nation in foreign affairs to conduct warrantless surveillance for intelligence purposes to detect and disrupt armed attacks on the United States."[4]

It is also important to note that there are statutory authorizations of the Executive Branch's foreign intelligence authority. Following the end of World War II, President Harry Truman sought authority to reorganize certain military departments, as well as create a full-time intelligence capability. The National Security Act of 1947 did just that, and it is also an important source of authority for certain Executive Branch agencies in the foreign intelligence space. The law has been amended by the USA Patriot Act; in 2004 by the Intelligence Reform and Terrorism Prevention Act of 2004, which is when the position of the director of National Intelligence was created; and the National Security Intelligence Reform Act of 2004.

Among the achievements of the National Security Act are:

- Reorganizing the IC.
- Reorganizing and creating the Department of Defense.
- Establishing the National Security Council.
- Establishing the Central Intelligence Agency.
- Establishing the position of DNI, who serves as the head of the IC, overseeing and directing the implementation of the National Intelligence Program and acting as the principal advisor to the president, National Security Council and Homeland Security Council for intelligence matters related to the national security.

- Establishing the National Counterterrorism Center to serve as a multiagency center analyzing and integrating all intelligence pertaining to terrorism, including threats to U.S. interests at home and abroad (implementing a key "9/11 Commission" recommendation).
- Mandating the development of procedures for the disclosure of foreign intelligence information acquired in criminal investigations and notice of criminal investigations of foreign intelligence sources.
- Mandating the development of procedures for access to classified information.
- Providing for presidential and congressional oversight of intelligence activities.[5]

The act in its original form also made an important distinction that we have seen carried through other statutes, including FISA, as well as in the activities of the IC—a distinction between foreign and domestic intelligence. Under the act, the newly created CIA had the authority to conduct clandestine activities for foreign intelligence gathering, but it would not have police, subpoena, or law enforcement powers, and the Federal Bureau of Investigation received the authority to conduct domestic intelligence operations. This distinction and the differences in the legal standards are discussed below.

This authority has been frequently used in the past, and this illustrates one of the common misconceptions—that, when President Jimmy Carter signed FISA in 1978, it created the authority for the Executive Branch to conduct foreign surveillance. As is illustrated by the Senate Report that accompanied FISA, as well as the findings of the Church Committee, nothing could be further from the truth.

The Church Committee was a Senate Committee that examined some of the abuses by the Executive Branch that had previously occurred with warrantless surveillance, and the Church Committee's findings were the reason FISA was proposed. The purpose of FISA was simple: to regulate the already-existing foreign intelligence practices.[6] Indeed, the Senate Report noted the testimony of Attorney General Bell regarding the importance of FISA:

> *"As Attorney General Bell stated in testifying in favor of the bill: I believe this bill is remarkable not only in the way it has been developed, but also in the fact that for the first time in our society the clandestine intelligence activities of our government shall be subject to the regulation and receive the positive authority of a public law for all to inspect.[7]"*

The Senate Report then identified several findings of the Church Committee that addressed prior Executive Branch Conduct:

> *"Since the 1930's, intelligence agencies have frequently wiretapped and bugged American citizens without the benefit of judicial warrant . . . [P]ast subjects of these surveillances have included a United States Congressman, Congressional staff member, journalists and newsmen, and numerous individuals and groups who engaged in no criminal activity and who posed no genuine threat to the national security, such as two White House domestic affairs advisers and an anti-Vietnam War protest group.*

> * * * * *
>
> *The application of vague and elastic standards for wiretapping and bugging has resulted in electronic surveillance which, by any objective measure, were improper and seriously infringed the Fourth Amendment Rights of both the targets and those with whom the targets communicated. The inherently intrusive nature of electronic surveillance, moreover, has enabled the Government to generate vast amounts of information—unrelated to any legitimate government interest—about the personal and political lives of American citizens. The collection of this type of information has, in turn, raised the danger of its use for partisan political and other improper ends by senior administration officials."*[8]

Lest there be any doubt, the Senate Report noted that FISA was "designed, therefore, to curb the practice by which the Executive Branch may conduct warrantless electronic surveillance on its own unilateral determination that national security justifies it. At the same time, however, this legislation does not prohibit the legitimate use of electronic surveillance to obtain foreign intelligence information."[9]

It is also important to note that, despite the Executive Branch's power here, Congress also had a role in regulating the conduct:

> *"The basis for this legislation is the understanding—concurred in by the Attorney General—that even if the President has an 'inherent' constitutional power to authorize warrantless surveillance for foreign intelligence purposes, Congress has the power to regulate the exercise of this authority by legislating a reasonable warrant procedure governing intelligence surveillance."*[10]

These points are important to understand when one examines FISA or EOs regarding foreign intelligence, such as EO 12333. While EO 12333 may allocate executive authority regarding foreign intelligence and FISA may permit and regulate certain forms of foreign intelligence gathering, the authority of the Executive Branch is not truly derivative of EO 12333 or FISA, but rather results from both constitutional powers of the executive, as well as the National Security Act, thus at some level falling in the broader presidential power scenario outlined in "Youngstown." In essence, a distinction can—and probably should—be drawn between the president's authority noted above and the authority of an Executive Branch agency, which is typically drawn from some delegation or instruction by the president, such as an EO, legislation or other similar sources. While these two concepts intersect and are related, they are not the same, and to conflate them reflects a misunderstanding of the true source of the president's authority.

The Fourth Amendment and history of domestic versus foreign intelligence and warrantless wiretaps

Warrantless wiretap is not a new issue in this country, and it has been, at varying times, used for both foreign and domestic intelligence gathering. It is important to start by examining the Fourth Amendment, which has received interesting treatment from the courts in connection with privacy issues. It states:

> *"The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."*[11]

The Fourth Amendment has typically been viewed as limited privacy protection, tied to more general protections against improper gathering of specific, tangible items, though courts recently seem to be framing Fourth Amendment issues in the context of broader privacy concerns.[12] While the existence of constitutional of privacy is not questioned by courts, it is also clear that government interference with privacy rights is proper if permitted by the Constitution.[13]

> *"The ultimate question, therefore, is whether one's claim to privacy from government intrusion is reasonable in light of all the surrounding circumstances ... In considering the reasonableness of asserted privacy expectations, the Court has recognized that no single factor invariably will be determinative. Thus, the Court has examined whether a person invoking the protection of the Fourth Amendment took normal precautions to maintain his privacy-that is, precautions customarily taken by those seeking privacy. Similarly, the Court has looked to the way a person has used a location, to determine whether the Fourth Amendment should protect his expectations of privacy ... The Court on occasion also has looked to history to discern whether certain types of government intrusion were perceived to be objectionable by the Framers of the Fourth Amendment. And, as the Court states today, property rights reflect society's explicit recognition of a person's authority to act as he wishes in certain areas, and therefore should be considered in determining whether an individual's expectations of privacy are reasonable."*[14]

One of the first cases to address the issue was Olmstead v. United States, 277 U.S. 438 (1928). As noted by the majority in Olmstead, the government gathered information regarding an alleged conspiracy via surveillance:

> *"The information which led to the discovery of the conspiracy and its nature and extent was largely obtained by intercepting messages on the telephones of the conspirators by four federal prohibition officers. Small wires were inserted along the ordinary telephone wires from the residences of four of the petitioners and those leading from the chief office. The insertions were made without trespass upon any property of the defendants. They were made in the basement of the large office building. The taps from house lines were made in the streets near the houses."*[15]

While there was no question in the court's mind that the Fourth Amendment protected papers, the person and his house, the answer was different regarding certain communications.[16] In drawing a contrast between the former and latter categories of information, the court stated:

> *"The United States takes no such care of telegraph or telephone messages as of mailed sealed letters. The Amendment does not forbid what was done here. There was no searching. There was no seizure. The evidence was secured by the use of the sense of hearing and that only. There was no entry of the houses or offices of the defendants.*

> *By the invention of the telephone, fifty years ago, and its application for the purpose of extending communications, one can talk with another at a far distant place. The language of the Amendment cannot be extended and expanded to include telephone wires reaching to the whole world from the defendant's house or office. The intervening wires are not part of his house or office any more than are the highways along which they are stretched."*[17]

In concluding the Fourth Amendment did not apply, the court noted that the installation and use of technology made these communications not subject to the Fourth Amendment: "The reasonable view is that one who installs in his house a telephone instrument with connecting wires intends to project his voice to those quite outside, and that the wires beyond his house and messages while passing over them are not within the protection of the Fourth Amendment. Here those who intercepted the projected voices were not in the house of either party to the conversation."[18]

Apart from its holding, the case is also notable because it gave us Justice Louis Brandeis's famous dissent, which reaffirmed his belief in the right to be let alone.[19] However, this holding did not stand the test of time, at least in the context of domestic crimes.

In Katz, the Supreme Court considered whether it was proper for the FBI to install a listening and recording device outside a public payphone to gather evidence of alleged misconduct that did not involve foreign intelligence issues.[20] The court noted at the outset that the Fourth Amendment protects people, not places, and thus the propriety of this conduct rests on an analysis of an individual's privacy expectation. Thus, what a person exposes to the public will not be protected, even if in a traditionally protected environment, such as a home, but what a person seeks to preserve as private, even in a public area, will be protected.[21]

While not directly overruling Olmstead, the court concluded the doctrine that served as the basis for the Olmstead decision had been eroded by subsequent decisions and the FBI's installation of a listening device outside a public telephone, without a warrant, violated the Fourth Amendment.[22] The court invalidated the search, finding that it did not fall within one of the recognized exceptions to warrantless searches.[23]

This case, decided in 1967, in hindsight telegraphed some of the issues that the Supreme Court and Congress would have to address and that are discussed above regarding FISA. In footnote 23, the court expressly noted that Katz did not address whether a warrant was required for searches involving national security.[24] Justice Byron White, in a concurrence, went further, noting that wiretapping to protect national security has been done by a number of presidents.[25] White also noted his agreement with these actions, stating, "We should not require the warrant procedure and the magistrate's judgment if the President of the United States or his chief legal officer, the Attorney General, has considered the requirements of national security and authorized electronic surveillance as reasonable."[26]

The legislative response was that Congress then enacted Title III of the Omnibus Crime Control and Safe Streets Act, which ultimately became the Electronic Communications Privacy Act.[27] This law controlled the interception of wire and electronic communications in

connection with certain crimes but did not at the time address foreign intelligence collections, and in fact, in its original form, contained some language that the Executive Branch saw as an affirmation of its unilateral power to conduct foreign intelligence activities.[28]

Domestic national security issues, in contrast to the domestic criminal issues that were at issue in Olmstead and Katz, were the next topic addressed by the Supreme Court in United States v. United States District Court, 407 U.S. 297, (1972). This case draws an important distinction that is sometimes elusive—purely domestic "criminal" activity versus purely domestic "national security" issues that are also ultimately crimes, but also impact the security of the union.

The court recognized the weighty issue before it:

> *"The issue before us is an important one for the people of our country and their Government. It involves the delicate question of the President's power, acting through the Attorney General, to authorize electronic surveillance in internal security matters without prior judicial approval.*
>
> *Successive Presidents for more than one-quarter of a century have authorized such surveillance in varying degrees, without guidance from the Congress or a definitive decision of this Court. This case brings the issue here for the first time. Its resolution is a matter of national concern, requiring sensitivity both to the Government's right to protect itself from unlawful subversion and attack and to the citizen's right to be secure in his privacy against unreasonable Government intrusion."*

Importantly, while this case involved national security, it was a purely domestic organization and individuals that were being prosecuted.[29] This distinction proved critical, and it was one that the court noted quite directly.[30]

The court first noted that the president had inherent authority to protect the U.S., including through using electronic surveillance, and the use and sanction of such conduct without judicial oversight had a long, bipartisan history.[31] In a discussion that would foreshadow the debate around connecting the dots post-9/11, the court also noted that technological advances made the Executive Branch's job much harder.[32]

The court began its analysis with the Katz case, noting that it did not directly tie the Fourth Amendment into instances of actual physical trespass. The court noted that Katz "implicitly recognized that the broad and unsuspected governmental incursions into conversational privacy which electronic surveillance entails necessitate the application of Fourth Amendment safeguards."

While the court recognized "the constitutional basis of the President's domestic security role," it also concluded that this role must be exercised in a manner compatible with the Fourth Amendment. Given that this case involved a purely domestic plot, the court concluded that the Fourth Amendment required a warrant as, "[t]hese Fourth Amendment freedoms cannot properly be guaranteed if domestic security surveillances may be conducted solely within the discretion of the Executive Branch. The Fourth Amendment does not contemplate the executive officers of Government as neutral and disinterested magistrates."[33]

The importance of these cases, apart from demonstrating the long history of warrantless wiretaps and the president's power to protect the union, is to illustrate the distinctions between domestic crimes and domestic national security issues versus foreign national security issues, as these distinctions are ultimately relevant, including under laws such as FISA.

The Fourth Amendment applied

In applying this standard, courts have found certain disclosures to be inconsistent with a reasonable expectation of privacy, including with bank and other records, particularly where they have been disclosed to a third party.[34] This is also true in connection with records related to internet subscription information,[35] as well as information that is displayed on the internet.[36]

One issue that has surfaced in the privacy realm related to searches is a doctrine that permits the government to search areas that were already searched by private citizens.[37] In the internet context, this doctrine has been used to justify searches of otherwise protected areas on the internet. This can result from giving a password to a third party, thus defeating a claim of a reasonable expectation of privacy, or because the expectation of privacy can effectively be destroyed by a private search.[38]

The Supreme Court has continued to address the Fourth Amendment as technology continues to advance and in so doing clarified the Fourth Amendment jurisprudence that flows from Katz. The Fourth Amendment analysis that has been the basis of many decisions has always been centered around whether there was a reasonable expectation of privacy. However, in Jones, the Supreme Court held that the Katz test was not the exclusive test under the Fourth Amendment, finding that the Fourth Amendment was rooted in property and notions of common-law trespass and that history justified a finding that the police needed a warrant before placing a geolocation device on a suspect's car.[39] This was true, despite prior case law that held that there was no reasonable expectation of privacy that would require a warrant before using a beeper or other similar device to track someone's public movements.

Though it did not directly decide the issue, the court noted that this conclusion might be different if there was no physical intrusion required to track—for example, the use of a cellphone to track a suspect's whereabouts.

This case does not change the reasonable expectation test but instead appears to offer two alternative tests that can require law enforcement to obtain a warrant, particularly if there is some form of intrusion on property.

The Leon warrant exception and wiretap warrants

While warrants are typically required under the Fourth Amendment, there are exceptions, including the good-faith exception to the general warrant requirement, which resulted from the Supreme Court's holding in U.S. v. Leon, 468 U.S. 897, 104 S. Ct. 3430, 82 L. Ed. 2d 677 (1984). While this exception was created by the courts to address issues under the Fourth Amendment, it is not explicitly referenced in the ECPA, which has its own warrant requirements, setting exclusion from evidence as the consequence of the violation of the ECPA's warrant requirement.[40] The 7th, 8th and 11th Circuits have previously held that the Leon good-faith exception applies to warrants under the ECPA.[41] However, the 6th Circuit

reached a different conclusion, relying upon the express text of 18 U.S.C.A. §2515, finding there is no good-faith exception to the warrant requirement in the ECPA and therefore excluding the evidence at issue in that case.[42]

EO 12333 and surveillance pre- and post-9/11

Executive Order 12333 is an important piece in the foreign intelligence puzzle in the U.S. Originally enacted in 1981, it has been amended by EOs 13284 (2003), 13355 (2004) and 13470 (2008). The EO does not create surveillance authority in the Executive Branch but rather reflects the president setting standards and regulating conduct, setting forth collection techniques, including restrictions on them, delegating authority to certain agencies, and setting forth goals for the IC. The EO mainly deals with foreign intelligence collection techniques of the U.S. government when acting abroad.[43] Though the EO does address certain FISA activities involving certain members of the IC, EO is an independent basis for foreign intelligence activities, apart from FISA.

EO 12333 provides the basis for certain surveillance activities abroad that are in addition to the acts that are regulated by FISA. In essence, EO 12,333 addresses the collection techniques of the U.S. in which the activities are undertaken abroad.[44]

The EO recognizes that "Timely, accurate, and insightful information about the activities, capabilities, plans, and intentions of foreign powers, organizations, and persons, and their agents, is essential to the national security of the United States" and that the need for this information must be balanced against the need to protect the legal rights of all U.S. people, including their freedoms, civil liberties and privacy rights under federal law. That is what the EO attempts to do. At its core, the purpose of the EO is:

> *"to enhance human and technical collection techniques, especially those undertaken abroad, and the acquisition of significant foreign intelligence, as well as the detection and countering of international terrorist activities, the spread of weapons of mass destruction, and espionage conducted by foreign powers."*[45]

The NSC and DNI

The EO states that the National Security Council shall serve as the highest-ranking executive branch entity to provide the president with "review of, guidance for, and direction to the conduct of all foreign intelligence, counterintelligence, and covert action, and attendant policies and programs."[46] The NSC is to submit policy recommendations to the president on all proposed covert actions, as well as do periodic reviews of covert actions, including for legal compliance.[47]

Subject to the authority, direction and control of the president, the director of National Intelligence serves as the head of the IC, the principle adviser to the president, NSC and Homeland Security Council for intelligence matters related to national security.[48] Moreover, the DNI has other duties, including budgetary responsibility.[49]

Duties of the IC

The EO also sets forth the duties of the Intelligence Community. Consistent with applicable federal law and other provisions of the EO and under the leadership of the DNI the IC shall:

- Collect and provide information needed by the president and, in the performance of executive functions, the vice president, NSC, Homeland Security Council, chairman of the Joint Chiefs of Staff, senior military commanders and other executive branch officials and, as appropriate, Congress.
- In accordance with priorities set by the president, collect information concerning and conduct activities to protect against international terrorism, proliferation of weapons of mass destruction, intelligence activities directed against the U.S., international criminal drug activities, and other hostile activities directed against the U.S. by foreign powers, organizations, people and their agents.
- Analyze, produce and disseminate intelligence.
- Conduct administrative, technical and other support activities within the U.S. and abroad necessary for the performance of authorized activities, to include providing services of common concern for the IC as designated by the director in accordance with this order.
- Conduct research, development and procurement of technical systems and devices relating to authorized functions and missions or the provision of services of common concern for the IC.
- Protect the security of intelligence-related activities, information, installations, property and employees by appropriate means, including such investigations of applicants, employees, contractors and other persons with similar associations with the IC elements as are necessary.
- Consider state, local and tribal governments' and, as appropriate, private sector entities' information needs relating to national and homeland security.
- Deconflict, coordinate and integrate all intelligence activities and other information gathering in accordance with Section 1.3(b)(20) of this order.
- Perform such other functions and duties related to intelligence activities as the president may direct.[50]

There are also a variety of duties imposed upon the heads of Executive Branch departments and agencies, as well as on the heads of Elements of the IC.[51] The individual IC entities each have individually imposed duties and responsibilities.[52] For example, the director of the CIA must:

- Collect (including through clandestine means), analyze, produce and disseminate foreign intelligence and counterintelligence.
- Conduct counterintelligence activities without assuming or performing any internal security functions within the U.S.
- Conduct administrative and technical support activities within and outside the U.S. as necessary for cover and proprietary arrangements.
- Conduct covert action activities approved by the president. No agency except the CIA (or the Armed Forces of the U.S. in time of war declared by the Congress or during any period covered by a report from the president to the Congress consistent with the War Powers Resolution, Public Law 93-148) may conduct any covert action activity unless the president determines that another agency is more likely to achieve a particular objective.
- Conduct foreign intelligence liaison relationships with intelligence or security services of foreign governments or international organizations consistent with Section 1.3(b)(4) of this order.
- Under the direction and guidance of the director and in accordance with Section 1.3(b)(4) of this order, coordinate the implementation of intelligence and counterintelligence rela-

tionships between elements of the IC and the intelligence or security services of foreign governments or international organizations.
- Perform such other functions and duties related to intelligence as the director may direct.[53]

The director of the NSA must:

- Collect (including through clandestine means), process, analyze, produce and disseminate signals intelligence information and data for foreign intelligence and counterintelligence purposes to support national and departmental missions.
- Establish and operate an effective unified organization for signals intelligence activities, except for the delegation of operational control over certain operations that are conducted through other elements of the IC. No other department or agency may engage in signals intelligence activities except pursuant to a delegation by the secretary of defense, after coordination with the director.
- Control signals intelligence collection and processing activities, including assignment of resources to an appropriate agent for such periods and tasks as required for the direct support of military commanders.
- Conduct administrative and technical support activities within and outside the U.S. as necessary for cover arrangements.
- Provide signals intelligence support for national and departmental requirements and for the conduct of military operations.
- Act as the national manager for National Security Systems as established in law and policy, and in this capacity, be responsible to the secretary of defense and director.
- Prescribe, consistent with Section 102A(g) of the act, within its field of authorized operations, security regulations covering operating practices, including the transmission, handling and distribution of signals intelligence and communications security material within and among the elements under control of the director of the NSA, and exercise the necessary supervisory control to ensure compliance with the regulations.
- Conduct foreign cryptologic liaison relationships in accordance with Sections 1.3(b)(4), 1.7(a)(6) and 1.10(i) of this order.[54]

The intelligence elements of the FBI must, under the supervision of the attorney general and any such regulations as the attorney general, may establish:

- Collect (including through clandestine means), analyze, produce and disseminate foreign intelligence and counterintelligence to support national and departmental missions, in accordance with procedural guidelines approved by the attorney general, after consultation with the director.
- Conduct counterintelligence activities.
- Conduct foreign intelligence and counterintelligence liaison relationships with intelligence, security and law enforcement services of foreign governments or international organizations in accordance with Sections 1.3(b)(4) and 1.7(a)(6) of this order.[55]

The Office of the Director of National Intelligence must collect (overtly or through publicly available sources), analyze, produce and disseminate information, intelligence and counter-

intelligence to support the missions of the ODNI, including the National Counterterrorism Center, and other national missions.[56]

One final thing to note is the role of the Department of Homeland Security, which is included in Section 1.7(i), among other agencies. DHS neither has a covert intelligence gathering function nor a national security role.

There are a variety of other duties set forth in EO 12333 for other agencies, but those will be covered in future discussions of the individual IC entity.

Conduct of intelligence activities

The IC is authorized to collect, retain or disseminate information concerning U.S. people only in accordance with procedures established by the head of the IC element concerned or by the head of a department containing such element and approved by the attorney general, consistent with the authorities provided by Part 1 of the EO, after consultation with the director. Those procedures shall permit collection, retention and dissemination of the following types of information:

- Information that is publicly available or collected with the consent of the person concerned.
- Information constituting foreign intelligence or counterintelligence, including such information concerning corporations or other commercial organizations. Collection within the U.S. of foreign intelligence not otherwise obtainable shall be undertaken by the FBI or, when significant foreign intelligence is sought, by other authorized elements of the IC, provided that no foreign intelligence collection by such elements may be undertaken for the purpose of acquiring information concerning the domestic activities of U.S. people.
- Information obtained in the course of a lawful foreign intelligence, counterintelligence, international drug or international terrorism investigation.
- Information needed to protect the safety of any persons or organizations, including those who are targets, victims or hostages of international terrorist organizations.
- Information needed to protect foreign intelligence or counterintelligence sources, methods and activities from unauthorized disclosure. Collection within the U.S. shall be undertaken by the FBI except that other elements of the IC may also collect such information concerning present or former employees, present or former intelligence element contractors or their present or former employees, or applicants for such employment or contracting.
- Information concerning people who are reasonably believed to be potential sources or contacts for the purpose of determining their suitability or credibility.
- Information arising out of lawful personnel, physical or communications security investigation.
- Information acquired by overhead reconnaissance not directed at specific U.S. people.
- Incidentally obtained information that may indicate involvement in activities that may violate federal, state, local or foreign laws.
- Information necessary for administrative purposes.[57]

Collection techniques

Elements of the IC shall use the least intrusive collection techniques feasible within the U.S. or directed against U.S. people abroad. Elements of the IC are not authorized to use such techniques as electronic surveillance, unconsented physical searches, mail surveillance,

physical surveillance or monitoring devices unless they are in accordance with procedures established by the head of the IC element concerned or the head of a department containing such element and approved by the attorney general, after consultation with the director. Such procedures shall protect constitutional and other legal rights and limit use of such information to lawful governmental purposes.

There are certain activities that were prohibited, including:

- The CIA engaging in electronic surveillance within the U.S. except for the purpose of training, testing or conducting countermeasures to hostile electronic surveillance.
- Unconsented physical searches in the U.S. by elements of the IC other than the FBI, except for: (1) Searches by counterintelligence elements of the military services directed against military personnel within the U.S. or abroad for intelligence purposes, when authorized by a military commander empowered to approve physical searches for law enforcement purposes, based upon a finding of probable cause to believe that such people are acting as agents of foreign powers; and (2) searches by CIA of personal property of non-U.S. people lawfully in its possession.
- Physical surveillance of a U.S. person in the U.S. by elements of the IC other than the FBI, except for: (1) Physical surveillance of present or former employees, present or former intelligence element contractors or their present or former employees, or applicants for any such employment or contracting; and (2) physical surveillance of a military person employed by a non-intelligence element of a military service.
- Physical surveillance of a U.S. person abroad to collect foreign intelligence, except to obtain significant information that cannot reasonably be acquired by other means.[58]

Attorney general approval for the FBI

The attorney general had authority delegated by the president to approve the use, for intelligence purposes, within the U.S. or against a U.S. person abroad, of any technique for which a warrant would be required if undertaken for law enforcement purposes, provided that such techniques shall not be undertaken unless the attorney general has determined in each case that there is probable cause to believe that the technique is directed against a foreign power or an agent of a foreign power. Electronic surveillance, as defined in FISA, shall be conducted in accordance with that act, as well as this order.[59]

It should be noted that this power does not exist with other members of the IC, and it only relates to U.S. people or activities in the U.S.

There are a variety of other standards and restrictions, including participation in organizations unless certain criteria are met, as well as certain limitations on covert actions.

Pre-9/11 surveillance by the NSA

Prior to 9/11 and the resulting president's Surveillance Program, as well as the later changes to FISA, the NSA was engaging in Signals Intelligence gathering against terrorists. This was done under its authority under EO 12333, and the communications that were gathered were only foreign communications, which was defined by the NSA as "communications having at least one communicant outside the United States, communications entirely among foreign powers,

or communications between a foreign power and officers or employees of a foreign power." Any other communications were "domestic communications," and the NSA was not authorized under E.O. 12333 to collect communications from a wire in the U.S. without a court order "unless the communications originated and terminated outside the United States or met applicable exceptions to the requirement of a court order under FISA."[60] In other words, it appears that the NSA could collect a communication that was between two individuals, both of whom were in foreign countries, even if the communication was, at some point, on a U.S. wire.

The president's surveillance program

In response to the terrorist attacks of September 11, 2001, on October 4, 2001, President George W. Bush issued a top-secret authorization to the secretary of defense directing that the signals intelligence (SIGNINT) capabilities of the NSA be used to detect and prevent further attacks in the U.S. The Presidential Authorization stated that an extraordinary emergency existed permitting the use of electronic surveillance within the U.S. for counterterrorism purposes, without a court order, under circumstances. This program has been known as the president's Surveillance Program, as well as its code name, STELLARWIND.[61]

This program was renewed on 30- to 60-day intervals for a number of years, and under this program, the NSA intercepted the content, as well as metadata of both U.S. and non-U.S. people.[62] In essence, this permitted the collection of communications where at least one person was in the U.S.[63] Content collection and analysis was done by the NSA in the same way it had conducted surveillance previously under E.O. 12333—standard minimization and procedures, as well as the use of selectors were used, and in this case the selector "had to be limited to al-Qa'ida, an associate, or international terrorism."[64] Regarding metadata, the NSA collected it "in bulk" under this program. Ultimately, the metadata program was run under Section 215 of FISA.

The president's Surveillance Program was the subject of intense legal scrutiny, as well as debate. It is important to note because the program started the surveillance under Section 215 and 702 of FISA that ultimately gained significant attention.

PPD-28

Presidential Policy Directive 28 was issued to address certain issues regarding surveillance, including certain principles involving foreign nationals and collection of intelligence. Specifically, PPD-28 states, "all persons should be treated with dignity and respect, regardless of their nationality or wherever they might reside, and all persons have legitimate privacy interests in the handling of their personal information." Additionally, PPD-28 notes that, "In determining why, whether, when, and how the United States conducts signals intelligence activities, we must weigh all of these considerations in a context in which information and communications technologies are constantly changing."

PPD-28 then sets forth principles regarding the collection of intelligence:

- The collection of signals intelligence shall be authorized by statute, EO, proclamation or other presidential directive and undertaken in accordance with the Constitution and applicable statutes, EOs, proclamations and presidential directives.

- Privacy and civil liberties shall be integral considerations in the planning of U.S. signals intelligence activities. The U.S. shall not collect signals intelligence for the purpose of suppressing or burdening criticism or dissent or for disadvantaging persons based on their ethnicity, race, gender, sexual orientation or religion. Signals intelligence shall be collected exclusively where there is a foreign intelligence or counterintelligence purpose to support national and departmental missions and not for any other purposes.
- The collection of foreign private commercial information or trade secrets is authorized only to protect the national security of the U.S. or its partners and allies. It is not an authorized foreign intelligence or counterintelligence purpose to collect such information to afford a competitive advantage to U.S. companies and U.S. business sectors commercially.
- Signals intelligence activities shall be as tailored as feasible. In determining whether to collect signals intelligence, the U.S. shall consider the availability of other information, including from diplomatic and public sources. Such appropriate and feasible alternatives to signals intelligence should be prioritized.[65]

PPD-28 also limited the use of "bulk collection" and added further refinements to the signals intelligence process.[66] There are also safeguards requirements, minimization requirements and other requirements contained within PPD-28, and certain of the requirements are directly tied to requirements of EO 12333.[67] Overall, it provides additional protections to foreign nationals who may be impacted by intelligence gathering by the U.S.

ECPA

The ECPA consists of the Wiretap Act and Stored Communications Act. The individual portions of the ECPA are sometimes referred to as Title I of the act, the Wiretap Act, which exclusively applies to the interception of communications, and Title II, the SCA, which applies to the dissemination or review of stored communications.[68]

Title I only applies to conduct that occurs at the precise time of transmission.[69] This is in contrast to conduct that violates Title II, which relates to the improper acquisition of the contents of stored communications (i.e. after their transmission).[70] Thus, the difference between the two titles is a temporal one. Title I applies only to the interception or accessing of information while in transmission, while Title II applies to the unauthorized access of storage communications.[71]

These acts regulate when electronic communications can be monitored or reviewed by third parties, including internet service providers. Generally, it is a crime for people to intercept or procure electronic communications,[72] which includes email and other electronic messages and transmissions, unless certain exceptions apply.[73] These include: (1) if the communication is made through a system that is readily accessible to the general public;[74] (2) to protect the rights or property of the provider, although random monitoring cannot be done;[75] (3) if a provider of electronic communication service reviews a communication to record the fact that a wire or electronic communication was initiated or completed if the purpose is to protect the provider, another provider, or a user, from fraudulent, unlawful or abusive use of the service;[76] (4) by court order;[77] (5) if the originator or addressee of any communication consents to the disclosure;[78] (6) a person employed or authorized, or whose facilities are used, to forward such communication to its destination (including employers);[79] or (7) if a communication is inadvertently obtained and the communication appears to pertain to the commission of a crime, if the communication is divulged to law enforcement.[80]

It is important to understand that the SCA was enacted to help limit government access to consumers' content because existing limits did not exist and provide methods for the regulation of government requests for information.[81] In addition to warrants, there were two other main methods for the government to obtain the content of communications: Section 2703(b) and Section 2703(d).

Obtaining subscriber information

Information about subscribers, other than content, can generally be obtained without a warrant—an administrative subpoena under Section 2703(c)(2), which does not require a neutral magistrate or probable cause, is sufficient.

Warshak and Section 2703(b)

Section 2703(b) of the SCA permitted, on its face, the government to obtain certain content from "remote computing services" without a warrant. The 6th Circuit addressed whether this was constitutional, ultimately concluding that 18 U.S.C.A. §2703(b) was unconstitutional because it violated the Fourth Amendment.[82] In Warshak, the government attempted to obtain emails from a remote computing service under the ECPA, without a warrant. Since the communications were in storage for more than 180 days, the government obtained a court order under Section 2703(b) permitting disclosure. Warshak objected to the government's attempts to get his emails and sought an injunction, arguing that this portion of the ECPA violated his Fourth Amendment rights. The government argued that it did not need to meet the probable cause standard to obtain emails via a court order, because the request for emails was not a search under the Fourth Amendment. Instead, the government's position was that it need only show that the emails were "reasonably relevant."[83] Though the ruling only applies to one circuit, the Department of Justice has agreed, as a matter of policy, to follow the Warshak holding generally and seeks warrants to obtain this type of content.

Section 2703(d) orders

The SCA also offers another path for the government to obtain the content of communications—a court order that is not a warrant, but more than a Section 2703(b) request. A court order for disclosure of the contents of communications or subscriber information can be issued if the governmental entity offers specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication or the records or other information sought are relevant and material to an ongoing criminal investigation.[84] In the case of a state governmental authority, such a court order cannot issue if prohibited by the law of the state.[85] A court issuing an order pursuant to this section, on a motion made promptly by the service provider, may quash or modify such order, if the information or records requested are unusually voluminous in nature or compliance with such order otherwise would cause an undue burden on the provider.[86]

FISA—an overview

The Foreign Intelligence Surveillance Act is an often cited and frequently misunderstood, law. It was the outgrowth of concern over unchecked surveillance within the U.S., and was designed to address the concerns raised before of the Church Committee, which were noted in prior articles.[87] What is perhaps the most important point is that even though FISA is focused

on "foreign intelligence" collections, its true focus is on regulating a subset of those collections—foreign intelligence collections that potentially impact U.S. people, or "domestic" collections—certain intelligence gathering that occurs in the U.S. FISA does not regulate all foreign intelligence gathering and, in fact, is not always the exclusive authority for foreign intelligence gathering by U.S. agencies authorized to carry out such activities.

FISA originally just covered electronic surveillance, but it has been repeatedly amended and expanded over the years, including an amendment signed by President Bill Clinton that authorized physical searches. Many amendments were also made in the wake of 9/11, and some of that authority remains. Moreover, over time, the use of pen registers and trap-and-trace devices was also later added to FISA.

FISA is broken down into a number of subchapters, and these subchapters are helpful in understanding the scope of FISA, as well as some of the limitations—they are Electronic Surveillance; Physical Searches; Pen Registers and Trap and Trace Devices for Foreign Intelligence Purposes; Access to Certain Business Records for Foreign Intelligence Purposes; Oversight; Additional Procedures Regarding Certain Persons Outside the United States; and Protection of Persons Assisting the Government. However, these labels can be a bit misleading because some of the electronic capture of data, including the prior "bulk collection" of metadata, occurs under the business records portion of FISA.

Another point to understand about FISA—there are a number of shortcuts and nicknames for statutes that practitioners frequently use, and Section 215 is a good example, which refers to the tangible records authority under 50 USC 1861. Another example is 50 USC Section 1881, also known as Section 702 of FISA. As these are discussed, the shortcuts will be introduced and used.

What and who does FISA cover?

The definitions of FISA matter, and it is through those definitions we begin to understand the scope of FISA. As noted previously, in the U.S. distinctions are drawn between intelligence gathering within the U.S. and intelligence gathering outside the U.S. Another key distinction that is recognized in FISA is against whom the surveillance occurs, a U.S. person people, as defined under the law,[88] or otherwise. In other words, the "who" and the "where" matter a lot.

Two key definitions that help understand the "who" are "foreign power" and "agent of a foreign power." Under FISA a "foreign power" is:

- A foreign government or any component thereof, whether or not recognized by the U.S.
- A faction of a foreign nation or nations, not substantially composed of U.S. people.
- An entity that is openly acknowledged by a foreign government or governments to be directed and controlled by such foreign government or governments.
- A group engaged in international terrorism or activities in preparation therefor.
- A foreign-based political organization, not substantially composed of U.S. people.
- An entity that is directed and controlled by a foreign government or governments.
- An entity not substantially composed of U.S. people that is engaged in the international proliferation of weapons of mass destruction.[89]

Another definition that is important to understand is who is an "agent of a foreign power." There are two definitions in FISA, one for non-U.S. people and one that includes U.S. people. The first is any person other than a U.S. person, who:

- Acts in the United States as an officer or employee of a foreign power or a member of a foreign power as defined in Subsection (a)(4), irrespective of whether the person is inside the U.S.
- Acts for or on behalf of a foreign power that engages in clandestine intelligence activities in the U.S. contrary to the interests of the U.S., when the circumstances indicate that such person may engage in such activities or when such person knowingly aids or abets any person in the conduct of such activities or knowingly conspires with any person to engage in such activities.
- Engages in international terrorism or activities in preparation therefore.
- Engages in the international proliferation of weapons of mass destruction or activities in preparation therefore.
- Engages in the international proliferation of weapons of mass destruction or activities in preparation therefore for or on behalf of a foreign power, or knowingly aids or abets any person in the conduct of such proliferation or activities in preparation therefor, or knowingly conspires with any person to engage in such proliferation or activities in preparation therefore.

The other formulation is any person, which includes U.S. people, who:

- Knowingly engages in clandestine intelligence gathering activities for or on behalf of a foreign power, which activities involve or may involve a violation of the criminal statutes of the U.S.
- Pursuant to the direction of an intelligence service or network of a foreign power, knowingly engages in any other clandestine intelligence activities for or on behalf of such foreign power, which activities involve or are about to involve a violation of the criminal statutes of the U.S.
- Knowingly engages in sabotage or international terrorism or activities that are in preparation therefore for or on behalf of a foreign power.
- Knowingly enters the U.S. under a false or fraudulent identity for or on behalf of a foreign power or, while in the U.S., knowingly assumes a false or fraudulent identity for or on behalf of a foreign power.
- Knowingly aids or abets any person in the conduct of activities described in Subparagraph (A), (B) or (C) or knowingly conspires with any person to engage in activities described in Subparagraph (A), (B), or (C).

It is important to note the distinctions here. The first definition, which excludes U.S. people, is broader and less tied to criminal violations of U.S. law. It is important to understand this in context because although FISA requests may not follow all of the traditional Fourth Amendment requirements, some probable cause elements are inherent because of the definition of "an agent of a foreign power," which is used for U.S. people, particularly when coupled with some of the prior judicial review that occurs under FISA.[90]

Another key point is the definition of "foreign intelligence information" under FISA. It is defined as:

- "information that relates to, and if concerning a United States person is necessary to, the ability of the United States to protect against—
  - actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power;
  - sabotage, international terrorism, or the international proliferation of weapons of mass destruction by a foreign power or an agent of a foreign power; or
  - clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power; or

- information with respect to a foreign power or foreign territory that relates to, and if concerning a United States person is necessary to—
  - the national defense or the security of the United States; or
  - the conduct of the foreign affairs of the United States."

The entities that are subject to Section 702 are "electronic communication service providers," which is defined as:

- A telecommunications carrier, as that term is defined in Section 153 of Title 47.
- A provider of electronic communication service, as that term is defined in Section 2510 of Title 18.
- A provider of a remote computing service, as that term is defined in Section 2711 of Title 18.
- Any other communication service provider that has access to wire or electronic communications either as such communications are transmitted or stored.
- An officer, employee or agent of an entity described in Subparagraph (A), (B), (C) or (D).[91]

A final key definition to focus on is "electronic surveillance." That term is defined as:

- "the acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire or radio communication sent by or intended to be received by a particular, known United States person who is in the United States, if the contents are acquired by intentionally targeting that United States person, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes;
- the acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire communication to or from a person in the United States, without the consent of any party thereto, if such acquisition occurs in the United States, but does not include the acquisition of those communications of computer trespassers that would be permissible under section 2511(2)(i) of title 18;
- the intentional acquisition by an electronic, mechanical, or other surveillance device of the contents of any radio communication, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes, and if both the sender and all intended recipients are located within the United States; or

- the installation or use of an electronic, mechanical, or other surveillance device in the United States for monitoring to acquire information, other than from a wire or radio communication, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes."

Again, it is important to note that these definitions all either relate to the collection of communications where at least one person is a U.S. person or the acquisition occurs in the U.S. where a person has a reasonable expectation of privacy and a warrant would be required. 50 USC Section 1812 reinforces this point, as it notes that, except as otherwise provided in FISA, the procedures in the Wiretap Act, SCA, Pen Register Act and FISA are the exclusive means by which electronic surveillance, and the interception of domestic (i.e. carried out within the U.S.) wire, oral or electronic communications may be conducted.[92]

But perhaps more important to this analysis is what the Senate report that accompanied FISA stated about this definition. When discussing the definition of an electronic communication in the original bill, the Senate noted that FISA would not apply to many of the surveillance activities outside the U.S., and this geographic limitation was done to avoid the regulation of certain activities conducted by the NSA, as well as other foreign surveillance activities.[93] In fact, the government has made clear that EO 12333 provides an independent basis for surveillance, including "human and technical collection techniques *** undertaken abroad."[94]

Each of the collection authorities will be discussed in future articles, but the important point about FISA overall is that it is a law that is targeted at protecting the rights of U.S. people, so it typically applies to collections that could impact U.S. people in certain circumstances or collections that are domestic. For surveillance that involves neither a U.S. person nor intelligence gathering within the boundaries of the U.S., FISA does not apply and therefore does not operate to govern or restrict that activity. In other words, the "who" and "where" matter for FISA.

Electronic surveillance under FISA

The original portion of FISA—Title 1—permits electronic surveillance in certain circumstances, both without and with a court order.

FISA—Electronic surveillance authorization without court order

Notwithstanding any other law, the president, through the attorney general, may authorize electronic surveillance without a court order under this subchapter to acquire foreign intelligence information for periods of up to one year if the attorney general certifies in writing under oath that:

- "the electronic surveillance is solely directed at—
    - the acquisition of the contents of communications transmitted by means of communications used exclusively between or among foreign powers, as defined in section 1801(a)(1), (2), or (3) of this title; or

- the acquisition of technical intelligence, other than the spoken communications of individuals, from property or premises under the open and exclusive control of a foreign power, as defined in section 1801(a)(1), (2), or (3) of this title;

- there is no substantial likelihood that the surveillance will acquire the contents of any communication to which a United States person is a party; and
- the proposed minimization procedures with respect to such surveillance meet the definition of minimization procedures under section 1801(h) of this title; and
- if the Attorney General reports such minimization procedures and any changes thereto to the House Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence at least thirty days prior to their effective date, unless the Attorney General determines immediate action is required and notifies the committees immediately of such minimization procedures and the reason for their becoming effective immediately."[95]

An electronic surveillance authorized by this subsection may be conducted only in accordance with the attorney general's certification and the minimization procedures adopted by him.[96]

Surveillance with a court order

Applications are to be made to the FISA Court, and each application for an order approving electronic surveillance under this subchapter shall be made by a federal officer in writing upon oath or affirmation. Each application shall require the approval of the attorney general based upon his finding that it satisfies the criteria and requirements of such application as set forth in this subchapter. It shall include:

- The identity of the federal officer making the application.
- The identity, if known, or a description of the specific target of the electronic surveillance.
- A statement of the facts and circumstances relied upon by the applicant to justify his belief that:

  - The target of the electronic surveillance is a foreign power or an agent of a foreign power.
  - Each of the facilities or places at which the electronic surveillance is directed is being used or is about to be used by a foreign power or an agent of a foreign power.

- A statement of the proposed minimization procedures.
- A description of the nature of the information sought and the type of communications or activities to be subjected to the surveillance.
- A certification or certifications by the assistant to the president for National Security Affairs, an executive branch official or officials designated by the president from among those executive officers employed in the area of national security or defense and appointed by the president with the advice and consent of the Senate or the deputy director of the FBI, if designated by the president as a certifying official:

  - That the certifying official deems the information sought to be foreign intelligence information.
  - That a significant purpose of the surveillance is to obtain foreign intelligence information.
  - That such information cannot reasonably be obtained by normal investigative techniques

- That designates the type of foreign intelligence information being sought according to the categories described in Section 1801(e) of this title.
- Including a statement of the basis for the certification that:

  - The information sought is the type of foreign intelligence information designated.
  - Such information cannot reasonably be obtained by normal investigative techniques.

- A summary statement of the means by which the surveillance will be affected and a statement whether physical entry is required to affect the surveillance.
- A statement of the facts concerning all previous applications that have been made to any judge under this subchapter involving any of the persons, facilities or places specified in the application and the action taken on each previous application.
- A statement of the period of time for which the electronic surveillance is required to be maintained, and if the nature of the intelligence gathering is such that the approval of the use of electronic surveillance under this subchapter should not automatically terminate when the described type of information has first been obtained, a description of facts supporting the belief that additional information of the same type will be obtained thereafter.[97]

Upon an application made pursuant to Section 1804, the judge shall enter an ex parte order as requested or as modified approving the electronic surveillance if he finds that:

- The application has been made by a federal officer and approved by the attorney general.
- On the basis of the facts submitted by the applicant there is probable cause to believe that:

  - The target of the electronic surveillance is a foreign power or an agent of a foreign power provided that no U.S. person may be considered a foreign power or an agent of a foreign power solely upon the basis of activities protected by the First Amendment to the Constitution.
  - Each of the facilities or places at which the electronic surveillance is directed is being used or is about to be used by a foreign power or an agent of a foreign power.

- The proposed minimization procedures meet the definition of minimization procedures under Section 1801(h) of this title.
- The application that has been filed contains all statements and certifications required by Section 1804 of this title and, if the target is a U.S. person, the certification or certifications are not clearly erroneous on the basis of the statement made under Section 1804(a)(7)(E) of this title and any other information furnished under Section 1804(d) of this title.[98]

An order approving an electronic surveillance under this section shall direct:

- That the minimization procedures be followed.
- That, upon the request of the applicant, a specified communication or other common carrier, landlord, custodian or other specified person, or in circumstances where the court finds, based upon specific facts provided in the application, that the actions of the target of the application may have the effect of thwarting the identification of a specified person, such other persons, furnish the applicant forthwith all information, facilities or technical

assistance necessary to accomplish the electronic surveillance in such a manner as will protect its secrecy and produce a minimum of interference with the services that such carrier, landlord, custodian or other person is providing that target of electronic surveillance.
- That such carrier, landlord, custodian or other person maintain under security procedures approved by the attorney general and DNI any records concerning the surveillance or the aid furnished that such person wishes to retain.
- That the applicant compensate, at the prevailing rate, such carrier, landlord, custodian or other person for furnishing such aid.[99]

There are also certain timing restrictions, as well as the ability to get emergency orders.[100] Civil immunity is available for certain individuals who furnish information, facilities or technical assistance pursuant to a court order or a request for emergency assistance.[101]

Sections 215 and 702

FISA Section 215/50 USC Section 1861

Section 215 is one of the more well-known provisions of FISA, though it is less likely to be the center of attention in the future, in light of recent amendments. Though 215 is not an electronically focused statute, but rather a statute directed to the production of "tangible things," it is best known for serving as the basis of the bulk metadata collection program.

In its current form, Section 215 permits the FBI to make an application for an order requiring the production of "any tangible things (including books, records, papers, documents, and other items) for an investigation to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution." Moreover, an investigation conducted under 215 must be conducted under guidelines approved by the attorney general under EO 12333.[102]

There are a number of restrictions on Section 215 requests, some of which are part of the recent FISA amendments. First, any request for tangible things must be made by the director of the FBI or a designee of the director whose rank can be no lower than assistant special agent in charge. However, for certain classes of records, the delegation cannot be below the deputy director or executive assistant director for national security. Second, these requests must be made to a judge on the FISA Court or certain designated magistrate judges.[103]

Third, these are not simply blanket requests for data but rather requests that relate to specific "selection terms," or selectors. As noted above, the "bulk collection" of telephony metadata that has been talked about in the media occurred under 215, but bulk collection was prohibited under 215 as a results of recent amendments to FISA. Fourth, 215 requires the creation of certain "minimization procedures," which are:

- Specific procedures that are reasonably designed in light of the purpose and technique of an order for the production of tangible things to minimize the retention and prohibit the dissemination of nonpublicly available information concerning unconsenting U.S.

people consistent with the need of the U.S. to obtain, produce and disseminate foreign intelligence information.
- Procedures that require that non-publicly available information, which is not foreign intelligence information, as defined in Section 1801(e)(1) of this title, shall not be disseminated in a manner that identifies any U.S. person, without such person's consent, unless such person's identity is necessary to understand foreign intelligence information or assess its importance.
- Notwithstanding the first two points, procedures that allow for the retention and dissemination of information that is evidence of a crime which has been, is being or is about to be committed and that is to be retained or disseminated for law enforcement purposes.[104]

These orders are typically made on an ex parte basis, though they can be subject to challenge by a recipient, as discussed below. They can also be made on an emergency basis, if certain criteria are met.[105]

An order under 215 must use a specific selector that meets the requirements of 1861(b)(2), as well as:

- Describe the tangible things that are ordered to be produced with sufficient particularity to permit them to be fairly identified, including each specific selection term to be used as the basis for the production.
- Include the date on which the tangible things must be provided, which shall allow a reasonable period of time within which the tangible things can be assembled and made available.
- Provide clear and conspicuous notice of the principles and procedures described in Subsection (d).
- Only require the production of a tangible thing if such thing can be obtained with a subpoena duces tecum issued by a court of the U.S. in aid of a grand jury investigation or with any other order issued by a court of the U.S. directing the production of records or tangible things.
- Not disclose that such order is issued for purposes of an investigation described in Subsection (a).
- In the case of an application described in Subsection (b)(2)(C):

    - Authorize the production on a daily basis of call detail records for a period not to exceed 180 days.
    - Provide that an order for such production may be extended upon application under Subsection (b) and the judicial finding under Paragraph (1) of this subsection.
    - Provide that the government may require the prompt production of a first set of call detail records using the specific selection term that satisfies the standard required under Subsection (b)(2)(C)(ii).
    - Provide that the government may require the prompt production of a second set of call detail records using session-identifying information or a telephone calling card number identified by the specific selection term used to produce call detail records under Clause (iii).
    - Provide that, when produced, such records be in a form that will be useful to the government.
    - Direct each person the government directs to produce call detail records under the order to furnish the government forthwith all information, facilities or technical

assistance necessary to accomplish the production in such a manner as will protect the secrecy of the production and produce a minimum of interference with the services that such person is providing to each subject of the production.
    - Direct the government to:

- Adopt minimization procedures that require the prompt destruction of all call detail records produced under the order that the government determines are not foreign intelligence information.
- Destroy all call detail records produced under the order as prescribed by such procedures.

There are certain restrictions on recipients of 215 requests. Specifically, a recipient of a 215 request cannot disclose to any other person that the FBI made a request other than to:

- Those persons to whom disclosure is necessary to comply with such order or such emergency production.
- An attorney to obtain legal advice or assistance with respect to the production of things in response to the order or the emergency production.
- Other persons as permitted by the director of the FBI or the designee of the director.[106]

A recipient who decides to challenge a 215 request may seek judicial review by filing a petition, which must immediately be assigned to a FISA judge to hear the case. The judge must do an initial review of the petition within 72 hours, and there may be additional proceedings. These proceedings are under seal, and there are appellate rights to the FISA Court of Review, as well as to the Supreme Court.[107]

It should also be noted that recent amendments to FISA either required or permitted, depending on the circumstances, amicus counsel.[108]

FISA Section 702/50 USC Section 1881a

The provision of FISA that has gotten the most attention, other than 215, is Section 702, or 18 USC § 1881a. Two programs—PRISM (also known as Downstream) and Upstream—that exist under Section 702 illustrate its importance and what Section 702 is used for. There are three key components to a 702 request: the certification that is discussed below, the authorization that is then permitted to conduct surveillance, and the directive, which is the method that is used to compel a third-party to provide information.

Section 702 permits the attorney general and the DNI to jointly and annually certify the criteria for Section 702 requests, and the criteria are then approved by the FISA Court, though the follow-on targeted requests or authorizations are not. From there, the government must meet the criteria of the certification, as well as other criteria, but it is then authorized to seek metadata and content regarding the targets of the surveillance. These targets are not supposed to be in the U.S. or U.S. people reasonably believed to be abroad. The government can also compel U.S. companies to assist them with these requests via a directive.

The certification

The first place to start with Section 702 is to understand the certification process that is a core part of Section 702. In short, while the FISA Court approves the certification, it does not approve the individual acquisitions of content, unlike certain other parts of FISA.

Prior to the implementation of an authorization or directive to a U.S. company, the attorney general and DNI must provide to the FISA Court a written certification and any supporting affidavit under oath and under seal.[109] The certification must:

- Attest that:
    - There are procedures in place that have been approved, have been submitted for approval, or will be submitted with the certification for approval by the Foreign Intelligence Surveillance Court that are reasonably designed to:
        - Ensure that an acquisition authorized under Subsection (a) is limited to targeting persons reasonably believed to be located outside the U.S.
        - Prevent the intentional acquisition of any communication as to which the sender and all intended recipients are known at the time of the acquisition to be located in the U.S.
    - The minimization procedures to be used with respect to such acquisition:
        - Meet the definition of minimization procedures under Section 1801(h) or 1821(4) of this title, as appropriate.
        - Have been approved, have been submitted for approval, or will be submitted with the certification for approval by the Foreign Intelligence Surveillance Court.
    - Guidelines have been adopted in accordance with Subsection (f) to ensure compliance with the limitations in Subsection (b) and that an application for a court order is filed as required by this chapter.
    - The procedures and guidelines referred to in Clauses (i), (ii), and (iii) are consistent with the requirements of the Fourth Amendment to the Constitution.
    - A significant purpose of the acquisition is to obtain foreign intelligence information.
    - The acquisition involves obtaining foreign intelligence information from or with the assistance of an electronic communication service provider.
    - The acquisition complies with the limitations in Subsection (b).
- Include the procedures adopted in accordance with Subsections (d) and (e).
- Be supported, as appropriate, by the affidavit of any appropriate official in the area of national security who is:
    - Appointed by the president, by and with the advice and consent of the Senate.
    - The head of an element of the IC.

- Include:
    - An effective date for the authorization that is at least 30 days after the submission of the written certification to the court.
    - If the acquisition has begun or the effective date is less than 30 days after the submission of the written certification to the court, the date the acquisition began or the effective date for the acquisition.

- If the attorney general and DNI decide under Subsection (c)(2), include a statement that such determination has been made.[110]

There are also requirements to adopt targeting procedures, minimization procedures and guidelines for compliance with limitations.

Once the certification is approved, surveillance against individuals is authorized. However, even after the certification is approved there are additional limitations that apply. Specifically, an acquisition that has been authorized:

- May not intentionally target any person known at the time of acquisition to be located in the U.S.
- May not intentionally target a person reasonably believed to be located outside the U.S. if the purpose of such acquisition is to target a particular, known person reasonably believed to be in the U.S.
- May not intentionally target a U.S. person reasonably believed to be located outside the U.S.
- May not intentionally acquire any communication as to which the sender and all intended recipients are known at the time of the acquisition to be located in the U.S.
- Shall be conducted in a manner consistent with the Fourth Amendment to the Constitution.[111]

Moreover, an approved acquisition pursuant to an approved certification can only be conducted in accordance the targeting and minimization procedures adopted in accordance with Subsections (d) and (e) and the terms of the approved certification.[112]

In other words, the FISA Court provides a preapproval review in the form of a review and approval of the certification but 702 does not require a review of the specific request on a case-by-case basis, though there is a process for challenging such a request.

Once surveillance is authorized, it is accomplished by the U.S. government providing selectors, such as an email address, to a U.S.-based company, consistent with the requirements of the certification and 702. The two programs that are public—PRISM (or Downstream) and Upstream—are important to understand when looking at Section 702. The programs accomplish similar goals but target different forms of electronic communications service providers. PRISM is a program in which U.S. service providers that are not telecommunications "backbone" companies, such as the more traditional internet companies. Upstream differs in that the request is sent to U.S. companies that are part of the telecommunications backbone.

Under PRISM, the NSA traditionally provides a "to or from" selector, such as an email address. In essence, this means the NSA is getting communications to or from the person tied to the selector. Under Upstream, the NSA has provided "to, from, or about" selectors, meaning that in addition, the NSA has collected communications "about" a target that were sent by others who were not the individual tied to the selector of a 702 request. In April 2017, the NSA announced that it would no longer be seeking internet communications based upon "abouts" requests.[113] However, amendments to FISA permit the resumption of these requests if certain criteria are met. These amendments also require additional burdens on the government related to incidentally collected 702 information that is collected about U.S. people, as well as certain limitations on the reuse of FISA information in criminal cases involving U.S. people.

Recipients of directives and rights of challenge

Once an acquisition is authorized and the selectors are provided, the attorney general or DNI can compel an electronic communications service provider, as defined by FISA, to help the government to fulfill a Section 702 request, and this is done via a directive. There is also a right to compensation, as well as a release from liability for providing information.[114]

One fundamental point about Section 702 requests is that a recipient of a request under Section 702 cannot reveal the existence of the request, particularly to the target.[115] However, the electronic communications service provider does have the right to challenge the directive it receives, though this does not include the right to challenge the certification.[116] The FISA Court will review the directive, and there is a right of appeal to the FISCR, as well as the Supreme Court. However, these challenges are done without the knowledge of the target of the surveillance.[117]

Endnotes

1 Juvenal, Satires (Satire VI, lines 347–348).

2 *Youngstown Sheet & Tube Co. v. Sawyer*, 343 U.S. 579, 635-637 (1952).

3 United States v. Brown, 484 F.2d 418 (5th Cir. 1973) ("As the *United States District Court* teaches, in the area of domestic security, the President may not authorize electronic surveillance without some form of prior judicial approval. However, because of the President's constitutional duty to act for the United States in the field of foreign relations, and his inherent power to protect national security in the context of foreign affairs, we reaffirm what we held in United States v. Clay, that the President may constitutionally authorize warrantless wiretaps for the purpose of gathering foreign intelligence."); *see also, United States v. Butenko*, 494 F.2d 593, (3rd Cir. 1974)(in a case involving activities of a foreign power, holding, "…that, in the circumstances of this case, prior judicial authorization was not required since the district court found that the surveillances of Ivanov were 'conducted and maintained solely for the purpose of gathering foreign intelligence information.'")

4 Legal Authorities Supporting the Activities of the National Security Agency Described by the President, January 19, 2006.

5 https://it.ojp.gov/PrivacyLiberty/authorities/statutes/1280

6 "The Federal Government has never enacted legislation to regulate the use of electronic surveillance in the United States for foreign intelligence purposes." Page 7.

7 Senate Report 95-604

8 Senate Report 95-604, citing (vol. 2, p. 12). (vol. 3, p. 32).

9 (Pg. 8.)

10 Pg. 16.

11 U.S. Const. Amend. IV.

12 Katz v. U.S., 389 U.S. 347, 350, 88 S. Ct. 507, 19 L. Ed. 2d 576 (1967) ("Secondly, the Fourth Amendment cannot be translated into a general constitutional 'right to privacy.' That Amendment protects individual privacy against certain kinds of governmental intrusion, but its protections go further and often have nothing to do with privacy at all. Other provisions of the Constitution protect personal privacy from other forms of governmental invasion.").

13 Katz v. U.S., 389 U.S. at 351, fn. 5 ("Virtually every governmental action interferes with personal privacy to some degree. The question in each case is whether that interference violates a command of the United States Constitution.").

14 Rakas v. Illinois, 439 U.S. 128, 152-153, 99 S. Ct. 421, 58 L. Ed. 2d 387 (1978) (citations omitted).

15 *Olmstead v. United States*, 277 U.S. 438, 456-57 (1928).

16 "The Amendment itself shows that the search is to be of material things — the person, the house, his papers or his effects. The description of the warrant necessary to make the proceeding lawful, is that it must specify the place to be searched and the person or things to be seized."

17 *Olmstead v. United States*, 277 U.S. 438, (1928).

18 *Olmstead v. United States*, 277 U.S. 438, (1928).

19 "[The makers of our Constitution] conferred, as against the government, the right to be let alone-the most comprehensive of rights and the right most valued by civilized men ... Subtler and more far-reaching means of invading privacy have become available to the government. Discovery and invention have made it possible for the government, by means far more effective than stretching upon the rack, to obtain disclosure in court of what is whispered in the closet." (Brandeis dissenting) Olmstead v. U.S., 277 U.S. 438, 48 S. Ct. 564, 72 L. Ed. 944, 66 A.L.R. 376 (1928) (overruled in part by, Berger v. State of N.Y., 388 U.S. 41, 87 S. Ct. 1873, 18 L. Ed. 2d 1040 (1967)) and (overruled in part by, Katz v. U.S., 389 U.S. 347, 88 S. Ct. 507, 19 L. Ed. 2d 576 (1967)).

20 Katz v. U.S., 389 U.S. 347, 88 S. Ct. 507, 19 L. Ed. 2d 576 (1967).

21 Katz v. U.S., 389 U.S. at 351.

22 Katz v. U.S., 389 U.S. at 353.

23 Citing Carroll v. U.S., 267 U.S. 132, 153, 156, 45 S. Ct. 280, 285, 286, 69 L. Ed. 543, 39 A.L.R. 790 (1925); McDonald v. U.S., 335 U.S. 451, 454-456, 69 S. Ct. 191, 192-194, 93 L. Ed. 153 (1948); Brinegar v. U.S., 338 U.S. 160, 174-177, 69 S. Ct. 1302, 1310-1312, 93 L. Ed. 1879 (1949); Cooper v. State of Cal., 386 U.S. 58, 87 S. Ct. 788, 17 L. Ed. 2d 730 (1967); Warden, Md. Penitentiary v. Hayden, 387 U.S. 294, 298-300, 87 S. Ct. 1642, 1645-1647, 18 L. Ed. 2d 782 (1967).

24 Katz v. U.S., 389 U.S. at 358, fn 23.

25 Katz v. U.S., 389 U.S. at 363.

26 Katz v. U.S., 389 U.S. at 364.

27 American Civil Liberties Union v. National Sec. Agency, 438 F. Supp. 2d 754, 16 A.L.R. Fed. 2d 749 (E.D. Mich. 2006), order vacated on other grounds, 493 F.3d 644 (6th Cir. 2007).

28 Pub. L. 90-351, 82 Stat. 211; American Civil Liberties Union v. National Sec. Agency, 438 F. Supp. 2d 754, 16 A.L.R. Fed. 2d 749 (E.D. Mich. 2006), order vacated on other grounds, 493 F.3d 644 (6th Cir. 2007).

29 "The affidavit also stated that the Attorney General approved the wiretaps to gather intelligence information deemed necessary to protect the nation from attempts of domestic organizations to attack and subvert the existing structure of the Government."

30 "Further, the instant case requires no judgment on the scope of the President's surveillance power with respect to the activities of foreign powers, within or without this country. The Attorney General's affidavit in this case states that the surveillances were [p309] "deemed necessary to protect the nation from attempts of domestic organizations to attack and subvert the existing structure of Government" (emphasis supplied). There is no evidence

of any involvement, directly or indirectly, of a foreign power."

31 "We begin the inquiry by noting that the President of the United States has the fundamental duty, under Art. II, § 1, of the Constitution, to "preserve, protect and defend the Constitution of the United States." Implicit in that duty is the power to protect our Government against those who would subvert or overthrow it by unlawful means. In the discharge of this duty, the President—through the Attorney General—may find it necessary to employ electronic surveillance to obtain intelligence information on the plans of those who plot unlawful acts against the Government. The use of such surveillance in internal security cases has been sanctioned more or less continuously by various Presidents and Attorneys General since July, 1946."

32 "Herbert Brownell, Attorney General under President Eisenhower, urged the use of electronic surveillance both in internal and international security matters on the grounds that those acting against the Government turn to the telephone to carry on their intrigue. The success of their plans frequently rests upon piecing together shreds of information received from many sources and many nests. The participants in the conspiracy are often dispersed and stationed in various strategic positions in government and industry throughout the country.

…

The marked acceleration in technological developments and sophistication in their use have resulted in new techniques for the planning, commission, and concealment of criminal activities. It would be contrary to the public interest for Government to deny to itself the prudent and lawful employment of those very techniques which are employed against the Government and its law-abiding citizens."

33 *United States v. United States District Court*, 407 U.S. 297, (1972).

34 Smith v. Maryland, 442 U.S. 735, 99 S. Ct. 2577, 61 L. Ed. 2d 220 (1979) (no reasonable expectation of privacy in the telephone numbers dialed by a telephone subscriber); U. S. v. Payner, 1980-2 C.B. 749, 447 U.S. 727, 731-32, 100 S. Ct. 2439, 65 L. Ed. 2d 468, 80-2 U.S. Tax Cas. (CCH) P 9511 (1980) (same for records given to a bank officer); U. S. v. Miller, 1976-1 C.B. 535, 425 U.S. 435, 96 S. Ct. 1619, 48 L. Ed. 2d 71, 76-1 U.S. Tax Cas. (CCH) P 9380, 37 A.F.T.R.2d 76-1261 (1976); see also U.S. v. White, 1971-1 C.B. 380, 401 U.S. 745, 91 S. Ct. 1122, 28 L. Ed. 2d 453 (1971) (no expectation of privacy in confidences exchanged in a private conversation).

35 U.S. v. Cox, 190 F. Supp. 2d 330, 332 (N.D. N.Y. 2002).

36 U.S. v. Gines-Perez, 214 F. Supp. 2d 205, 225 (D.P.R. 2002) ("[I]t strikes the Court as obvious that a claim to privacy is unavailable to someone who places information on an indisputably, public medium, such as the internet, without taking any measures to protect the information.")

37 U.S. v. D'Andrea, 648 F.3d 1, 7 (1st Cir. 2011), citing, U.S. v. Jacobsen, 466 U.S. 109, 115, 104 S. Ct. 1652, 80 L. Ed. 2d 85 (1984) ("The additional invasions of [a defendant's] privacy by the Government agent must be tested by the degree to which they exceeded the scope of the private search.")

38 *See*, U.S. v. Runyan, 275 F.3d 449, 464-465 (5th Cir. 2001); Paul v. State, 57 P.3d 698, 702-03 (Alaska Ct. App. 2002).

39 United States v. Jones, 132 S.Ct. 945, (2012).

40 18 U.S.C.A. §2515.

41 *See* U.S. v. Ning Wen, 477 F.3d 896 (7th Cir. 2007); U.S. v. Moore, 41 F.3d 370, 376 (8th Cir. 1994); U.S. v. Malekzadeh, 855 F.2d 1492, 1497 (11th Cir. 1988).

42 U.S. v. Rice, 478 F.3d 704, 2007 FED App. 0088P (6th Cir. 2007).

43 *See*, Brief for the Petitioners, *Clapper v. Amnesty International USA*, 2012 WL 3090949 (2012), citing S. Rep. No. 701, 95th Cong. 2d Sess. 71 (1978).

44 In theory the EO could, in other limited circumstances, apply to certain collections in the United States.

45 Section 2.2.

46 Section 1.2(a).

47 Section 1.2(b).

48 Section 1.3.

49 Section 1.3(a)-(b).

50 Section 1.4.

51 Section 1.5-1.6.

52 Section 1.7.

53 Section 1.7(a)(1)-(7).

54 Section 1.7(c)(1)-(8).

55 Section 1.7(g).

56 Section 1.7(j).

57 Section 2.3(a)-(j).

58 Section 2.4.

59 Section 2.5.

60 https://oig.justice.gov/reports/2015/PSP-09-18-15-vol-I.pdf

61 https://oig.justice.gov/reports/2015/PSP-09-18-15-vol-I.pdf

62 https://oig.justice.gov/reports/2015/PSP-09-18-15-vol-I.pdf

63 It appears that the authority was broader under the authorizations, but the NSA did not believe it should collect purely domestic communications, because the NSA is a foreign intelligence agency. https://oig.justice.gov/reports/2015/PSP-09-18-15-vol-I.pdf Pg. 9.

64 https://oig.justice.gov/reports/2015/PSP-09-18-15-vol-I.pdf Pg. 18.

65 PPD-28, Section 1.

66 PPD-28, Section 2-3.

67 PPD-28, Section 4.

68 Hall v. EarthLink Network, Inc., 396 F.3d 500 (2d Cir. 2005); Organizacion Jd Ltda. v. U.S. Dept. of Justice, 124 F.3d 354, 356 (2d Cir. 1997).

69 Steve Jackson Games, Inc. v. U.S. Secret Service, 36 F.3d 457 (5th Cir. 1994); U.S. v. Moriarty, 962 F. Supp. 217, 221 (D. Mass. 1997) (drawing temporal distinction between acquisition of communications during transmission under Title I and acquisition of contents of communications in a non-contemporaneous manner under Title II.).

70 Bohach v. City of Reno, 932 F. Supp. 1232, 1236-37, 11 I.E.R. Cas. (BNA) 1707 (D. Nev. 1996) (Electronic

communications are not intercepted when they are in electronic storage.).

71 U.S. v. Moriarty, 962 F. Supp. 217 (D. Mass. 1997).

72 "Electronic communication" is defined as any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce. 18 U.S.C.A. §2510(11).

73 18 U.S.C.A. §2511(1)(a).

74 18 U.S.C.A. §2511(2)(g)(1).

75 18 U.S.C.A. §2511(2)(a)(1).

76 18 U.S.C.A. §2511(2)(h)(ii).

77 18 U.S.C.A. §2511(2)(a)(ii)(A).

78 18 U.S.C.A. §2511(3)(b)(ii).

79 18 U.S.C.A. §2511(3)(b)(iii).

80 18 U.S.C.A. §2511(3)(b)(iv).

81 The SCA "was born from congressional recognition that neither existing federal statutes nor the Fourth Amendment protected against potential intrusions on individual privacy arising from illicit access to stored communications in remote computing operations and large data banks that stored e-mails." *In re Google Inc. Cookie Placement Consumer Privacy Litig.*, 806 F.3d 125, 145 (3d Cir. 2015).

82 Warshak v. U.S., 490 F.3d 455 (6th Cir. 2007), reh'g en banc granted, opinion vacated, (Oct. 9, 2007).

83 Warshak, 490 F.3d at 469.

84 18 U.S.C.A. §2703(d).

85 18 U.S.C.A. §2703(d).

86 18 U.S.C.A. §2703(d).

87 According to the Church Commission, "Since the 1930's, intelligence agencies have frequently wiretapped and bugged American citizens without the benefit of judicial warrant . . . [P]ast subjects of these surveillances have included a United States Congressman, Congressional staff member, journalists and newsmen, and numerous individuals and groups who engaged in no criminal activity and who posed no genuine threat to the national security, such as two White House domestic affairs advisers and an anti-Vietnam War protest group. (vol. 2, p. 12).

*****

The application of vague and elastic standards for wiretapping and bugging has resulted in electronic surveillance which, by any objective measure, were improper and seriously infringed the Fourth Amendment Rights of both the targets and those with whom the targets communicated. The inherently intrusive nature of electronic surveillance, moreover, has enabled the Government to generate vast amounts of information—unrelated to any legitimate government interest—about the personal and political lives of American citizens. The collection of this type of information has, in turn, raised the danger of its use for partisan political and other improper ends by senior administration officials. (vol. 3, p. 32)."

88 "United States person" means a citizen of the United States, an alien lawfully admitted for permanent residence (as defined in section 1101(a)(20) of title 8), an unincorporated association a substantial number of members of which are citizens of the United States or aliens lawfully admitted for permanent residence, or a corporation which is incorporated in the United States, but does not include a corporation or an association which is a foreign power, as defined in subsection (a)(1), (2), or (3). 50 U.S. Code § 1801(i)

89 50 USC § 1801(a).

90 For a comparison of the Title III and Fourth Amendment requirements, and FISA, *see, In re Sealed Case*, 310 F.3d 717 (2002).

91 50 U.S.C. § 1881(b)(4).

92 50 USC Section 1812(a)(emphasis added).

93 *See*, Brief for the Petitioners, *Clapper v. Amnesty International USA*, 2012 WL 3090949 (2012), citing S. Rep. No. 701, 95th Cong. 2d Sess. 71 (1978).

94 *Id.*, citing Exec. Order 12,333, Section 2.2, 3 C.F.R. 210 (1981 Comp.).

95 50 U.S.C.A. § 1802(a)(1).

96 50 U.S.C.A. § 1802(a)(2).

97 50 U.S.C.A. § 1804(a)(1)-(9).

98 50 U.S.C.A. § 1805(a)(1)-(4).

99 50 U.S.C.A. § 1805(c)(2)(A)-(D).

100 50 U.S.C.A. § 1805(d)-(f).

101 50 U.S.C.A. § 1805(i).

102 50 USC § 1861(a)(1)-(2).

103 50 USC § 1861(a)-(b).

104 50 USC § 1861(g)(1)-(2).

105 50 USC § 1861(c), (f), (i).

106 50 USC § 1861(d)(1).

107 50 USC § 1861(f)(2)-(3).

108 50 USC § 1803(i).

109 18 USC § 1881a(g). In certain limited circumstances a certification is not required. See 50 USC Section 1881a(g)(1)(B).

110 50 USC Section 1881a(g).

111 50 USC § 1881a(b).

112 50 USC § 1881a(c)(1).

113 https://www.nsa.gov/news-features/press-room/statements/2017-04-28-702-statement.shtml.

114 50 USC § 1881a(h)(1)-(3).

115 50 USC § 1881a(h)(1)(A)(giving the Attorney General and the DNI the authority to direct an electronic communications service provider to "immediately provide the Government with all information, facilities, or assistance necessary to accomplish the acquisition in a manner that will protect the secrecy of the acquisition and produce a minimum of interference with the services that such electronic communication service provider is providing to the target of the acquisition…")

116 50 USC § 1881a(4).

117 50 USC § 1881a(4), (6).