Seton Hall University
eRepository @ Seton Hall

Law School Student Scholarship | Seton Hall Law

2019

Government Surveillance and The War On Terror: Why is Government Cyber Data Collection Increasingly Sanctioned by the Courts, Despite The Development of Privacy Law Protections Against Domestic Surveillance Beginning in the Early Twentieth Century?

Ashley E. Morgan

Follow this and additional works at: https://scholarship.shu.edu/student_scholarship

Part of the Law Commons

Recommended Citation

Morgan, Ashley E., "Government Surveillance and The War On Terror: Why is Government Cyber Data Collection Increasingly Sanctioned by the Courts, Despite The Development of Privacy Law Protections Against Domestic Surveillance Beginning in the Early Twentieth Century?" (2019). *Law School Student Scholarship*. 1006.
https://scholarship.shu.edu/student_scholarship/1006

INTRODUCTION

The right to be free from unwarranted government intrusion is a product of the innate right of the individual to be left alone.[2] John Locke's theory of the social contract maintains that man surrendered some of their innate freedoms in order to share in the protection of the state.[3] This original sacrifice parallels the relationship between government intelligence agencies and individual citizens. National security concerns prompt the government to conduct covert surveillance in order to keep citizens safe, while individual privacy concerns lead to the rise of bureaucratic obstacles to combat excessive intrusions.

The relationship between the citizen and the state is constantly evolving in light of technological development. Technology's unprecedented expansion during industrialization, first prompted Samuel Warren and Louis Brandeis to issue a warning against technologies inevitable invasion into the "sacred precincts of private and domestic life."[4] Their article, "The Right to Privacy," asserts that at the heart of the liberty of the individual is "the more general right of the individual to be let alone."[5] Statutory regulations, such as defamation law and property law, provide inadequate means to alleviate privacy concerns, while the U.S. Constitution contains no express right to privacy. Warren and Brandeis, thus, called for a return to the common law as a means to develop an effective remedy for the preservation of citizens' privacy rights.

It wasn't until *Griswold v. Connecticut* in 1965, that Justice Douglas was able to articulate the legal foundations for judicially enforceable privacy protections.[6] Justice Douglas reasoned that the penumbras originating in the Bill of Rights give life and substance to the specific guarantees.[7]

---

[2] Peter Laslett, John Locke: Two Treatises of Government (1965).
[3] *Id.*
[4] *See* Daniel J. Solove, Marc Rotenberg & Paul M. Schwartz, *Information Privacy Law* 10 (2d ed. 2006).
[5] Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 Harv. L. Rev 193, 205 (1890).
[6] *Griswold v. Connecticut*, 381 U.S. 479 (1965).
[7] *Id.* at 484.

The Court determined that these various guarantees create "zones of privacy." In 1977, the Court further held, in *Whalen v. Roe*, that the constitutionally protected "zone of privacy" extends to two distinct types of interests: (1) "independence in making certain kinds of important decisions"; and (2) the "individual interest in avoiding disclosure of personal matters."[8] The latter interest has been called the "constitutional right to information privacy," as termed in *Nixon v. Administrator of General Services*, decided that same year.[9] Following *Whalen* and *Nixon*, the Court did not develop the right of information privacy. Nevertheless, a majority of circuit courts have recognized this right, which has been involved in a substantial number of cases.[10]

Although the courts acknowledge that there is a constitutional right to information privacy, it is limited when government data collection implicates national security. The Federal Government's seemingly unyielding ability to collect citizens' data under the guise of foreign intelligence gathering raises imperative privacy concerns. This paper proposes that information privacy laws are quickly growing antiquated, as rapid technological advancement revolutionizes both the tools available to the government for surveillance and those used by individuals to live their lives. Section I provides a general overview of how modern judicial standards for determining privacy protections developed in response to the government's utilization of telephone advancements to surveil citizens. Section II looks at how widespread public disapproval of domestic government surveillance prompted Congress to bolster information privacy protections through legislation that distinguished between domestic and foreign surveillance with the former being most strictly regulated.

---

[8] *Whalen v. Roe*, 433 U.S. 425, 599-600 (1977).
[9] *Nixon v. Adm'r of Gen. Servs.*, 433 U.S. 425 (1977)
[10] *See* Solove Et Al., *supra* note 61, at 401.

Specifically, Section III looks at the Foreign Intelligence Surveillance Act of 1978 (FISA) as the main means by which the Federal government meant to reign in unwarranted domestic surveillance that was not necessary for the promotion of national security. Section IV looks at information privacy protections in a post-9/11 society where the Patriot Act and other Presidential directives have been used to transform FISA into the main means by which the government justifies the data collection of citizen's information. Section V then reasons that information privacy protections, developed in a time of traditional warfare and prior to the advent of the internet, are inadequate to protect against warfare waged through cyberspace. This writing concludes that it is imperative that new information privacy laws be legislated in response to technological developments that are incompatible with current privacy protections. Without new legislation to provide judicial guidelines for enforcing privacy protections, the courts are left to operate within the constraints of laws designed to address antiquated technological surveillance and of a conception of national security that did not envision a war waged through cyberspace as opposed to through ground warfare. Ultimately, the government is taking advantage of the novelty of the War on Terror and cyberspace communications to re-envision vague conceptions of "foreign powers" described in FISA as justification for the collection of citizen's data.

I. JUDICIAL CONCEPTION OF FOURTH AMENDMENT PRIVACY PROTECTIONS AGAINST GOVERNMENT SURVEILLANCE

With the advent of industrialization, colonial fears of the rise of a tyrannical government resurfaced with advancements in technology to foster widespread public distrust of government surveillance. Historically, many colonial states had Peeping Tom laws that criminalized the spying

upon or invading the privacy of the persons spied upon.[11] These attitudes endured after the emergence of electronic eavesdropping with over half the states making wiretapping a crime by 1928.[12] On the other hand, federal surveillance laws were slower to respond to public privacy concerns. Consequently, it fell to the judiciary to interpret whether there existed adequate protections from government intrusion under the Fourth Amendment.

State courts were the first to take on the question of whether a right to privacy existed, and ultimately, found that there was a lack of existing precedent to find such a right. Accordingly, when the Supreme Court first tackled the legality of government surveillance in 1928 with *Olmstead v. United States*, they gave the government an essentially unyielding ability to conduct wiretapping activities as they could find intrusion of the citizen's home.[13] Wiretapping surveillance would not be labeled an unwarranted intrusion until the Court in *Katz v. United* made the distinction between public and private spheres of protection as a means for determining what is a citizen's reasonable expectation of privacy.[14] Finally, in 1972, *United States v. United States District Court for the Eastern District of Michigan, Southern Division*, placed specific limitations on the government's ability to conduct surveillance even when it concerns national security.[15] Nonetheless, the Court made clear that the provisions and protections in these rulings applied only to domestic surveillance operations, leaving little to no guidance for the surveillance of foreign powers or their agents.

---

[11] Daniel J. Solove, *A Taxonomy of Privacy*, 154 University of Pennsylvania Law Review 477, 491 (2006).
[12] *Id.* at 492.
[13] *Olmstead v. United States*, 277 U.S. 438 (1928).
[14] *Katz v. United States*, 389 U.S. 347 (1967).
[15] *United States v. United States District Court for the Eastern District of Michigan, Southern Division*, 407 U.S. 297 (1972).

A. PRIVACY TORTS AND THE RIGHT OF PROTECTION FROM INTRUSION UPON SECLUSION

Warren and Brandeis spoke of privacy as an intangible as opposed to a physical injury. Privacy, contended the authors, involves "injury to the feelings."[16] With their decision in *Roberson v. Rochester Folding Box Co.*, the New York Court of Appeals put states on notice that a lack of existing precedent for actions concerning invasions of privacy, prevented the judiciary from inventing an action as the courts were "without authority to legislate.[17] State legislatures compensated for the lack of existing judicial frameworks in dealing with threats to individual autonomy through the formation of privacy torts. In 1960, William Prosser analyzed the inundation of privacy cases spawned in the wake of Warren and Brandeis article to distinguish four distinct privacy torts: (1) intrusion upon seclusion; (2) public disclosure of private facts; false light or "publicity"; and (4) appropriation.[18] The protection against intrusion upon seclusion recognized a sphere of privacy where the individual is free from unwanted third-party surveillance.

It wasn't until 1965 that The *Restatement of Torts* would define intrusion upon seclusion as protecting against electronic eavesdropping into conversations in the home, as well as the deceitful entry and clandestine photographing of activities in the home.[19]The tort is not limited to intrusions into the home, but claims involving surveillance in public have generally not been successful. In certain instances, "surveillance may be so 'overzealous' as to render it actionable" as it can reveal hidden details that would not ordinarily be observed by others.[20] The court did not recognize the surveillance as harm itself, rather, their focus was more on the harm of disclosure

[16] Warren & Brandeis, *supra* note 21, at 197
[17] Roberson v. Rochester Folding Box Co., 64 N.E. 442, 442 (N.Y. 1902).
[18] William L. Prosser, *Privacy*, 48 Cal. L. Rev. 383 (1960).
[19] Restatement [Second] if Torts § 652B.
[20] *Nader v. General Motors Corp.*, 225 N.E.2d 765, 771 (N.Y. 1970).

that destroyed secrecy. Therefore, privacy protections hinged largely on whether states had passed their own privacy torts as they lacked any Supreme Court precedent or federal legislation that would support such a finding.

B. OLMSTEAD V. UNITED STATES

In 1928, the Supreme Court in *Olmstead v. United States* tackled the issue of whether the Fourth Amendment required a warrant before the government could engage in wiretapping.[21] The Court concluded that because "[t]here was no searching. There was no seizure. . . There was no entry of the houses or offices of the defendants," that the Fourth Amendment did not apply to wiretapping as it did not involve trespass inside a person's home.[22] In his dissent, Justice Brandeis alluded to his earlier "The Right of Privacy" article, reflecting his view that new technological developments necessitated revising traditional views of the Fourth Amendment in order to preserve its purpose of protecting privacy in light of such "far reaching" means.[23]

The *Olmstead* holding drew considerable aversion from the public, culminating six years later with Congress enacting section 605 of the Federal Communications Act of 1934 to blunt the effect of the Court's ruling.[24] With the expectation of making wiretapping a federal crime, the Act prohibits the interception and divulgence of any communication by an unauthorized third party.[25] The statute did not actually restrict officials from engaging wiretapping. It only prevented government officials from disclosing the intercepted communications in court proceedings.[26]

---

[21] *Olmstead v. United States*, 277 U.S. 438 (1928).
[22] *Id*. at 464.
[23] *Id*. at 473.
[24] Louis Fisher, *Congress and The Fourth Amendment*, 21 GA. L. Rev. 107, 127 (1986).
[25] Former 7 U.S.C. § 605.
[26] *Id*.

Together with *Olmstead*, the Act led to a significant increase of wiretapping by the FBI and state law enforcement officials.

C. KATZ V. UNITED STATES

The Court in *Katz v. United States* first made the distinction between varying zones of protection in determining what is a reasonable expectation of privacy.[27] Nearly four decades after *Olmstead*, the Court ushered in a Fourth Amendment resurgence through the "reasonable expectation of privacy test" established in *Katz*.[28] *Katz* involved the wiretapping of a telephone conversation made by the defendant while in a phone booth.[29] In overturning *Olmstead*, the Court distinguished between the public and private spheres, reasoning that "what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected."[30] Justice Harlan's concurrence, clarifies that, to determine whether an expectation of privacy is reasonable, the Court asks whether (1) a person exhibits an "actual or subjective expectation of privacy" and (2) "the expectation [is] one that society is prepared to recognize as 'reasonable.'"[31] Essentially, *Katz* provided an objective standard for the courts to determine what would be a socially accepted limitation on the government's ability to invade a citizen's right to privacy. Evidently, this limitation looks to what would be historically considered taking place within the "home," and that such expectation of privacy is reasonable in light of the competing demands of the citizen and the government.

---

[27] *Katz v. United States*, 389 U.S. 347 (1967).
[28] *Id.*
[29] *Id.*
[30] *Id.* at 351-52.
[31] *Id.* at 361 (Harlan, J., concurring).

One year later, Congress passed the Omnibus Crime Control and Safe Streets Act of 1968 as a means of codifying the limitations to government surveillance expounded in *Katz*.[32] Title III, of the Act, provided comprehensive protection against wiretapping by requiring law enforcement officials to obtain a warrant before wiretapping.[33] The scope was limited to domestic law enforcement purposes as it rested on a citizen's right to Fourth Amendment protections from unwarranted government intrusion.[34]Accordingly, in line with the Fourth Amendment requirement that there be notice of government searches, the existence of a Title III wiretap is disclosed to the subject of the surveillance after the fact.[35] As a result, more than just overturning *Olmstead*, the holding in *Katz* served as the impetus for constraining the government's ability to surveil citizens through the implementation of mandatory judicial safeguards.

D. UNITED STATES V. U.S. DISTRICT COURT

In 1972 the Court further limited the government's ability to conduct electronic surveillance with *United States v. United States District Court for the Eastern District of Michigan, Southern Division*, finding that the interests of national security do not override Fourth Amendment protections from unwarranted government intrusion.[36] The Court determined that the President may not authorize electronic surveillance of persons within the United States without first obtaining a judicial warrant.[37] Fourth Amendment freedoms cannot be properly guaranteed if

---

[32] Omnibus Crime and Control and Safe Streets Act of 1968, 18 U.S.C. §§ 2510-22.
[33] *See* Priscilla M. Regan, *Legislating Privacy: Technology, Social Values, and Public Policy* 46, note 114, at 122-25 (1995).
[34] Title III and FISA "shall be the exclusive means by which electronic surveillance . . . and the interceptions of domestic wire and oral communications may be conducted. 18 U.S.C. § 2511(2)(f).
[35] Title III requires notice "[w]ithin a reasonable time but not later than ninety days" after surveillance expires. 18 U.S.C. § 2518(8)(d).
[36] *United States v. United States District Court for the Eastern District of Michigan, Southern Division*, 407 U.S. 297 (1972).
[37] *Id.* at 321-22.

domestic security surveillance is to be conducted solely within the discretion of the Executive Branch.[38] This established the precedent that a warrant needed to be obtained before beginning electronic surveillance, even if domestic security issues were involved.

However, the Court stressed that this holding was limited to cases involving "the domestic aspects of national security," providing no opinion with regards to the surveillance of foreign powers or their agents.[39] This clarified *Katz*, in that Fourth Amendment protections from unwarranted government intrusion only apply to domestic surveillance and not the surveillance of foreign powers or their agents.[40] Even so, with this seemingly insignificant restraint, Congress was provided with the impetus to create a new judicial mechanism for overseeing government surveillance conducted in the name of national security. Accordingly, Congress split surveillance into two parts – the procedures of Title III a mentioned above, which would apply to ordinary crimes and domestic security wiretaps, and the special procedures of FISA, which would apply only to "agents of a foreign power."[41]

II. LEGISLATIVE RESPONSE TO PUBLIC INDIGNATION OVER MEDIA REVELATIONS ON DOMESTIC GOVERNMENT SURVEILLANCE

In 1975, public distrust of the federal government reached never before seen levels. Following on the heels of Watergate, Seymour Hersh revealed the CIA's role in not only undermining foreign government but in spying on U.S. citizens.[42] Congress responded with the creation of the Church Committee. A series of hearings held over sixteen months exposed the

---

[38] *Id.* at 316-17
[39] *Id.*
[40] *Id.* at 319-21.
[41] *See* Peter P. Swire, *The System of Foreign Intelligence Surveillance Law*, 72 The George Washington L. Rev. 1306, 1322 (2004).
[42] Seymour M. Hersh, *Huge C.I.A. Operation Reported in U.S. Against Antiwar Forces, Other Dissidents in Nixon Years*, N. Y. TIMES, Dec. 22, 1974, at 1.

unprecedented scope of the intelligence community's abuses over the previous decades and would forever alter the public's perception of the United States' intelligence agencies.[43] Reacting to the damaging conclusions in the Committee's reports, Legislatures sought to balance intelligence agencies' calls for maximum flexibility to protect national security, with the increasingly aggravated public's calls for new laws and institutions to prevent future abuses. The Committee's wide-ranging revelations prompted a wave of federal legislation that would permanently alter how intelligence agencies operate.

Beginning with the Privacy Act of 1974, Congress sought to address the increasing computerization of information through regulation of federal agencies seeking to access and collect such records.[44] The Act, while the first step in updating federal legislation to coincide with new technological advancements, lacked clear interpretations of various components which would later be exploited by the government in their attempts to push the boundaries of what is accepted under the Fourth Amendment. In the same way, the Electronic Communications Privacy Act of 1986 sought to extend many of the same protections available for "wire" and "oral" communications, to e-mail and other "electronic" communications.[45] Even so, while Congress appeared to acquiesce with public concerns, in reality their attempts at legislation were poorly done with much of the vague limitations left up to interpretation by the courts.

A. PRIVACY ACT OF 1974

[43] *Intelligence Activities: Hearing on S. Res. 21 Before the Select Comm. to Study Governmental Operations with Respect to Intelligence Activities of the United States*, 94th Cong. vol. 1-7 (1975).
[44] Privacy Act of 1974, Pub. L. No. 93-579, 88 Stat. 1896, 1896 (codified at 5 U.S.C. § 552a (2000)).
[45] 18 U.S.C §§ 2510–22, 2701–11, 3121–27.

Congress responded to the increasing computerization of information and the burgeoning repositories of personal data in federal agencies with the passage of the Privacy Act of 1974.[46]The Act regulates the collection and use of records by federal agencies by requiring them to "establish appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of records." [47] Essentially, this did nothing to prevent surveillance, but rather, addressed how surveillance should be properly conducted and granted individuals the right to access their personal information. Moreover, as the first legislative attempt at reigning in government information systems, the Act was limited in scope. It does not apply to the private sector, nor does it apply to state or local agencies.[48]

Most problematic was the inclusion of the "routine use" exception.[49] Information could be disclosed for any "routine use," if disclosure is "compatible" with the purpose for which the agency collected the information.[50] This exception effectively serves as a loophole to the requirement that a federal agency acquire the consent of the individual prior to disclosing their information to a third party. Instead, an otherwise unauthorized disclosure could be justified through a simple mechanical analysis of the relationship between the information disclosed and the routine use purported by the agency. Implicit in such an analysis is the court's acceptance of the published routine use as the "purpose" for which the information was collected. The lack of judicial standards for interpreting what constitutes a "routine use" and the secrecy that surrounds the motivations for intelligence gathering, effectively rendered the Act fruitless.

---

[46] Privacy Act of 1974, Pub. L. No. 93-579, 88 Stat. 1896, 1896 (codified at 5 U.S.C. § 552a (2000)).
[47] 5 U.S.C. § 522a(e)(10).
[48] 5 U.S.C. § 552a.
[49] 5 U.S.C. § 552a(b)(3).
[50] *Id.*

B. ELECTRONIC COMMUNICATIONS PRIVACY ACT OF 1986

Congress revisited its wiretapping law by substantially reworking Title III of 1968. The Electronic Communications Privacy Act (ECPA) restricts the interception of transmitted communications and the searching of stored communications.[51] Under the ECPA, Title III protections were expanded to new forms of communications, with a particular focus on computers.[52] Previously, Title III had applied to "wire" and "oral" communications, i.e., to phone wiretaps and bugs. The ECPA extended many of these same protections to email and other "electronic" communications.

Specifically, Title I of the ECPA, known as the "Wire-tap Act," regulates the interception of communications.[53] Title II, referred to as the "Stored Communications Act," governs access to stored communications and records held by communications service providers.[54] Title III, called the "Pen Register Act," provides limited regulation of pen registers and trap and trace devices.[55] Essential to the structure of Title III and ECPA is the requirement of judicial supervision of wiretaps, the need to give notice to the object of surveillance once the wiretap is completed, and the obligation to minimize the amount of surveillance in order to prevent intrusions that are outside of the law enforcement investigation.[56] Unlike the Privacy Act of 1974, ECPA was far more effective in providing concrete barriers to unwarranted government surveillance by expanding on existing framework as opposed to creating new and underdeveloped provisions.

---

[51] 18 U.S.C. §§ 2510–22, 2701-11.
[52] 18 U.S.C §§ 2510–22, 2701–11, 3121–27.
[53] 18 U.S.C. §§ 2510–22.
[54] 18 U.S.C. §§ 2701–11.
[55] 18 U.S.C. §§ 3121–27.
[56] 18 U.S.C. §§ 2510–22, 2701-11.

III. THE FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978 LIMITED DOMESTIC SURVEILLANCE WHILE EXPANDING FOREIGN INTELLIGENCE GATHERING

The Church Committee and other revelations of the 1970s had shown that the FBI had used the risk of "subversion" and other potential crimes as the justification for investigating a vast array of political and other domestic activity.[57] The Foreign Intelligence Surveillance Act (FISA) of 1978 was Congress's largest attempt to reconcile the judiciary's evolving zone of privacy jurisprudence with the continuing necessity for national security intelligence gathering.[58] The 1978 statute therefore specified that the application for a FISA order certify that "the purpose of the surveillance is to obtain foreign intelligence information."[59] FISA is meant to calm public fears through the collection of personal data under the guise of national security. Targets of FISA surveillance usually never learn they are the objects of government searches, and only one opinion from the Foreign Intelligence Surveillance Court of Review, *In Re Sealed Case*, has ever been published.[60]

Unlike the Privacy Act of 1974 or ECPA, FISA was focused on regulating foreign, as opposed to domestic, surveillance. FISA permits electronic surveillance and covert searches pursuant to courts orders, which are reviewed ex parte by a special court of seven federal judges.[61]

---

[57] See CHURCH FINAL REP. Ila, *supra* note 59 (noting that between 1960 and 1974, "subversion" alone was used to justify more than 500,000 investigations, with apparently no prosecutions for the actual crimes)
[58] Pub. L. No. 95-511, codified at 50 U.S.C. §§ 1801–11.
[59] 50 U.S.C. § 1804(7). This language was changed in 2001 to say that "a significant purpose of the investigation is to obtain foreign intelligence information." Uniting and Strengthening America by Providing Appropriate Tools to Intercept and Obstruct Terrorism (USA PATRIOT Act) Act of 2001, Pub. L. No. 107-56, § 218, 115 Stat. 272, 291 (codified at 50 U.S.C.A. § 1804(7) (West 2003)); see also infra Part IV.A.1.
[60] *In re* Sealed Case, 310 F.3d 717 (U.S. Foreign Intelligence Surveillance Ct. Rev. 2002).
[61] *Id.*

These judges are designated by the Chief Justice to the new Foreign Intelligence Surveillance Court (FISC).[62] These judges have jurisdiction to issue orders approving electronic surveillance upon finding a number of factors, notably if "there is probable cause to believe that the target of the electronic surveillance is a foreign power or an agent of a foreign power."[63] Essentially, FISA and FISC serve as a means by which the government can justify their surveillance as promoting national security, or else, be forced to abide by the normal Fourth Amendment constraints.

FISA revealed a grand compromise between the advocates for citizen's privacy rights and the intelligence community. From the citizen's privacy rights side, FISA had the advantage of creating a legal structure for foreign intelligence surveillance that involved Article III judges. It had the disadvantage of having standards that were less protective overall than were constitutionally and statutorily required for investigations of domestic crimes. Specifically, the notice requirement of the Fourth Amendment did not apply, and targets of FISA surveillance usually never learned they were the objects of government searches. From an efficiency standpoint, FISA had the disadvantage of imposing bureaucratic rules and procedures on searches that had previously been done subject to the inherent authority of the President or the Attorney General. An advantage was that FISA provided legislative legitimation for secret wiretaps and created standardized bureaucratic procedures for getting them. By establishing these clear procedures, it became easier over time for the number of FISA surveillance orders to grow.

A. FISA TAKES MANY OF ITS REGULATIONS FROM TITLE III, BUT ALSO INCORPORATES OVERSIGHT FROM OTHER BRANCHES OF GOVERNMENT AS A LIMITATION ON DOMESTIC SURVEILLANCE

[62] 50 U.S.C. § 1803
[63] 50 U.S.C. § 1805(a)(3)(A)

FISA orders contain some, but not all, of the other safeguards in Title III. Both regulations require mitigation to reduce the effects on persons other than the "targets" of surveillance.[64] Both provide for electronic surveillance for a limited duration, but afford an opportunity to extend the surveillance.[65] Both require facts concerning the targets of the surveillance and the nature and location of the facilities placed under surveillance.[66] Both allow "emergency" orders, where the surveillance can begin without judicial approval subject to quick, subsequent approval by a judge.[67] To regularize congressional oversight, the Attorney General must report to the House and Senate Intelligence Committees every six months about FISA electronic surveillance, including a description of each criminal case in which FISA information has been used for law enforcement purposes.[68] The Attorney General also must make an annual report to Congress and the public about the total number of applications made for orders and extensions of orders, as well as the total number that were granted, modified, or denied.[69] This report is similar to that required for Title III wiretaps, but the latter provides additional details such as the types of crimes for which a wiretap is used and the number of wiretaps that resulted in successful prosecutions.[70]

---

[64] *Compare* 50 U.S.C. § 1805(a)(4) (FISA applications), *with* 18 U.S.C. § 2518(5) (Title III applications).
[65] *Compare* 50 U.S.C. § 1805(e) (FISA applications), *with* 18 U.S.C. § 2518(5) (Title III applications).
[66] *Compare* 50 U.S.C. § 1805(c)(1) (FISA applications), *with* 18 U.S.C. § 2518(4) (Title III applications).
[67] FISA originally required judicial approval of an emergency order within twenty-four hours, but this was extended to seventy-two hours in 2001. Intelligence Authorization Act for Fiscal Year 2002, Pub. L. No. 107-108, § 314(a)(2)(B), 115 Stat. 1394, 1402 (2001) (codified at 50 U.S.C.A. § 1805(f) (West 2003)). Title III emergency orders must be approved by a judge within forty-eight hours. 18 U.S.C. § 2518(7).
[68] *See id.* § 1808(a). In the initial years after passage of FISA, the Intelligence Committees were additionally required to report to the full House and Senate about the operation of the statute. *Id.* § 1808(b).
[69] *Id.* § 1807.
[70] *See* 18 U.S.C. § 2529 (reports on Title III wiretaps); *see also* 18 U.S.C. § 3126 (2000) (reports on pen register and trap and trace orders).

In addition to Congressional oversight, Congress also relied on institutional structures within the executive branch to check overuse of domestic surveillance.[71] The requirement that the Attorney General authorize applications meant that the FBI on its own could no longer implement national security wiretaps. Applications by the FBI would need to be approved by the Justice Department. In light of the historical evidence about the independence of longtime FBI Director J. Edgar Hoover from control by the Justice Department, and the disagreements that have often continued between the FBI and the Department, this supervision by the Justice Department was a potentially significant innovation in FISA.[72]

Under Title III and the Fourth Amendment, surveillance is only authorized if there is a showing of probable cause that the surveillance will uncover evidence of criminal activity.[73] Title III gives discretion to the judge to refuse to issue the order, even where the statutory requirements have been met.[74] On the other hand, FISA orders are granted if there is probable cause to believe that the monitored party is a "foreign power" or "an agent of a foreign power."[75] Under FISA, the judge "shall" issue the order once the statutory findings are met.[76] FISA has looser standards about whether other, less-intrusive surveillance techniques must first be exhausted. FISA is applied when foreign intelligence gathering is "the purpose" of the investigation.[77] FISA process is cloaked in secrecy.

---

[71] 50 U.S.C. § 1805(a)(2).
[72] *See, e.g.*, Jeff Nesmith et al., *Subtle Forces Swirl Just Beneath Siege Inquires: The Tug of Personality Conflict in Washington Alters Flow of Waco Controversy*, AUSTIN AM.-STATESMAN, Sept. 19, 1999, at Al (discussing "tension" between the Department of Justice and the FBI, and between Attorney General Reno and FBI Director Freeh).
[73] 18 U.S.C. § 2518(3)(a) (2000).
[74] "Upon such application the judge may enter an ex parte order, as requested or as modified, authorizing or approving interception, ..." 18 U.S.C. § 2518(3) (emphasis added).
[75] 50 U.S.C. § 1801.
[76] 50 U.S.C. § 1805(a).
[77] *See* former 50 U.S.C. § 1804(a)(7)(B) prior to USA PATRIOT Act amendment in 2001.

Targets of FISA surveillance almost never learn that they have been subject to a wiretap or other observation. The only statutory exception is where evidence from FISA surveillance is used against an individual in a trial or other proceeding.[78] In such instances, the criminal defendant or other person can move to suppress the evidence on the grounds that the information was unlawfully acquired or the surveillance did not comply with the applicable order.[79] Even still, the individuals have no right to see the evidence against them. The secrecy and ex parte nature of FISA applications are a natural outgrowth of the statute's purpose, to conduct effective intelligence operations against agents of foreign powers.[80] Consequently, because the purpose of foreign surveillance is to promote national security, the government is granted far more flexibility in conducting their operations so as not to compromise safety.

B. FISA IS FOCUSED ON FOREGIN SURVEILLANCE AND THE GOVERNMENT'S NEED TO SAFEGUARD NATIONAL SECURITY

In contrast to most other federal legislation on government surveillance, FISA is aimed at foreign, rather than domestic, intelligence gathering. The Act drew distinctions between U.S. persons and non-U.S. persons.[81] The former consists fundamentally of U.S. citizens and permanent residents.[82] Non-U.S. persons could qualify as an "agent of a foreign power" simply by being an officer or employee of a foreign power, or a member of an international terrorist group.[83] Reacting to the historical evidence about surveillance of political speech and association, the 1978 statute provided that "no United States person may be considered a foreign power or an agent of a foreign

[78] 50 U.S.C. § 1806.
[79] *Id.*
[80] *See* 50 U.S.C. § 1802(a)(1)(A)(i).
[81] *Id.* § 1801(i).
[82] *Id.*
[83] *Id.* § 1801(b)(1)(A).

power solely upon the basis of activities protected by the first amendment to the Constitution of the United States.[84]This language reflects a congressional concern about infringement on First Amendment activities, but provides only modest safeguards, because an individual could apparently be considered an agent of a foreign power based "largely" or "substantially" on protected activities. The standards for surveillance against U.S. persons were stricter, in line with the Church Committee concerns about excessive surveillance against domestic persons. U.S. persons qualified as an "agent of a foreign power" only if they knowingly engaged in listed activities, such as clandestine intelligence activities for a foreign power, which "involve or may involve a violation of the criminal statutes of the United States.[85]

Similarly, "foreign powers" is broadly defined to include any "foreign government or any component thereof, whether or not recognized by the United States."[86] Surveillance could be conducted against an "agent of a foreign power" which traditionally meant a foreign intelligence operative, but could also include a person who "knowingly engages in sabotage or international terrorism, or activities that are in preparation therefor, for or on behalf of a foreign power."[87] This expansion on the traditional definition provided greater room for interpretation, and effectively, meant that the definition could potentially be expanded to include domestic citizens. Likewise, the definition of "international terrorism" had three elements: violent actions in violation of criminal laws; an intent to influence a government by intimidation or coercion; and actions that transcend nation boundaries in their method or aims."[88] The final definition can be applied that any action

[84] 50 U.S.C. § 1805(a)(3)(A).
[85] *Id.* § 1801(b)(2)(A).
[86]50 U.S.C. § 1801(a)(1).
[87] 50 U.S.C. § 1801(b)(2)(C).
[88] 50 U.S.C. § 1801(c). The term "international terrorism" was defined in full as:
[A]ctivities that-(1) involve violent acts or acts dangerous to human life that are a violation of the criminal laws of the United States or of any State, or that would be a criminal violation if committed within the jurisdiction of the United States or any State; (2) appear to be intended-(A) to intimidate or coerce a civilian population;

that involves the internet as cyberspace is not confined to any one location. Additionally, this can also be applied to our current War on Terror as it is not being waged against a specific nation-state but is being fought with an entity that has no national boundaries. Consequently, while these attempts to define foreign surveillance were meant to protect against incursions in domestic intelligence, they could not have foreseen that the advent of cyberspace and the War on Terror would make the distinction between the two realms incredibly murky.

IV. THE "WAR ON TERROR" TRANSFORMED FISA INTO A MEANS FOR SPYING ON CITIZENS UNDER THE GUISE OF NATIONAL SECURITY

In the wake of the unprecedented war on terror, the means used to wage war have responded with a growing emphasis on cyberspace surveillance. Post-9/11 national security initiatives and policies hasten this erosion of the zones of privacy through the necessary expansion of executive power to embolden intelligence data collection as a means to combat terrorism. Beginning with the USA PATRIOT ACT of 2001, the Federal Government took advantage of the ambiguities present in FISA and the ECPA to expand their surveillance programs to incorporate domestic data collection as an incidental result of their efforts to protect national security. Likewise, Presidential Policy Directives further expanded the government's authority to engage in cyber espionage as the main means for combating terrorism. These actions by the executive remove almost all accountability and further immerse the surveillance programs of federal agencies in a realm of secrecy. Thus, previously unassuming deficiencies in prior privacy legislation has allowed the Federal Government to create loopholes whereby they can conduct what amounts to essentially

(B) to influence the policy of a government by intimidation or coercion; or (C) to affect the conduct of a government by assassination or kidnapping; and (3) occur totally outside the United States or transcend national boundaries in terms of the means by which they are accomplished, the persons they appear intended to coerce or intimidate, or the locale in which their perpetrators operate or seek asylum.

domestic surveillance as a byproduct of their efforts to combat cyber security threats brought about by the War on Terror.

A. USA PATRIOT ACT OF 2001

Almost immediately after the terrorist attacks of September 11, Congress passed the "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act" (USA PATRIOT Act) of 2001. The Act provided for new justifications for delayed notice of search warrants, increasing the types of subscriber records that could be obtained from ISPs and communication providers, and allowing for search warrants for email.[89] The Act also provided for increased sharing of foreign intelligence information between law enforcement entities.[90] Most importantly, the Act made several significant changes to the ECPA and FISA, among other statutes. These changes effectively took advantage of the expanded definitions for "foreign powers" present within FISA to interpret them as applying to domestic citizens so long as their inclusion was merely incidental to the protection of national security.[91]

FISA's application was expanded to instances when foreign intelligence gathering is "a significant purpose" of the investigation as opposed to "the purpose."[92] Under Section 215 of the USA PATRIOT Act, the FISA court must grant any subpoena for any "tangible things that the FBI requests," so long as the FBI specifies that those things are "sought for" an investigation related to terrorism or spying.[93] The FBI need not show that the target of the investigation is engaged in spying, terrorism, or criminal activity, and the FBI may base its investigation at least in part on the

[89] *See* SOLOVE ET AL., *supra* note 61, at 294–300.
[90] *Id.* at 343.
[91] 50 U.S.C. § 1801(b)(2)(C).
[92] 50 U.S.C. § 1804(a)(7)(B) as amended by USA PATRIOT Act § 204.
[93] The Reauthorization Act requires that the FBI show "that there are reasonable grounds to believe" that the records sought are "relevant to an authorized investigation." H.R. 3199 § 106(b).

subject's First Amendment-protected activity.[94] Transitioning from "the purpose" to "a significant purpose" thus, allows for more than one justification to be proposed. Additionally, that justification need not be as well supported since it is not the end all of the investigation but rather one objective in a grand scheme.

In 2002, Attorney General John Ashcroft submitted to the FISA court new FISA investigation procedures that substantially diminished the "information screening wall" that had previously prevented law enforcement officials from initiating or directing FISA surveillance.[95] While the FISA court rejected the procedures, on appeal, the Foreign Intelligence Surveillance Court of Review reversed the FISA Court.[96] In its first and only published opinion, *In Re Sealed Case*, the court concluded that the USA PATRIOT Act "by using the word 'significant,' eliminated any justification for the FISA court to balance the relative weight the government places on criminal prosecution as compared to other counterintelligence responses.[97] In essence, this reversed the policy granting Freedom of Information Act (FOIA) requests to prevent some information from entering the public domain. There is a veil of secrecy that has fallen over the Federal Government, and now not only is transparency illusive, in some areas it is nonexistent.

B. PRESIDENTIAL POLICY DIRECTIVES

President Obama signed Presidential Policy Directive 20 (PPD-20) in October 2012 as a complement to President George W. Bush's Comprehensive National Cybersecurity Initiative

[94] If the target is a "United States person," the investigation may not be "conducted solely upon the basis of activities protected by the first amendment to the Constitution," Patriot Act §215. This makes it possible for such an investigation to be solely based upon the First Amendment protected activities of non-United States persons and to conduct investigations of United States persons based primarily, but not solely, upon First Amendment protected activities.
[95] Daniel J. Solove, A Brief History of Information Privacy Law in PROSKAUER ON PRIVACY, PLI (2006).
[96] *In re* All Matters Submitted to the Foreign Intelligence Surveillance Court (May 17, 2002).
[97] *In re* Sealed Case, 310 F.3d 717 (U.S. Foreign Intelligence Surveillance Ct. Rev. 2002).

launched in 2008, National Security Presidential Directive 54/Homeland Security Presidential Directive 23.[98] The initiative and its associated activities evolved to become key elements of a broader, updated national U.S. cybersecurity strategy.[99] PPD-20 provides a framework for United States cybersecurity through the establishment of principles and processes for "cyber collection operations that are reasonably likely to result in 'significant consequences.'"[100] The directive details government policy regarding offensive cyber action and instructions to compile a list of potential targets for such action. According to the classified document, the "Government shall identify potential targets of national importance where [cyberattacks] can offer a favorable balance of effectiveness and risk . . ."[101] The directive gives broader power to the military to block cyberattacks and discusses what constitutes an "offensive" verses a "defensive" action with respect to cyberwar and cyberterrorism.

In July 2016, President Obama also approved a Presidential Policy Directive 41, which established clear principles that will govern the Federal government's activities in cyber incident response.[102] The directive was focused on "significant cyber incidents."[103] Significant cyber incidents are those that will likely result in "demonstrable harm to the national security interests,

---

[98] Presidential Policy Directive 20, https://epic.org/privacy/cybersecurity/presidential-directives/presidential-policy-directive-20.pdf

[99] See, e.g., WHITE HOUSE, NATIONAL STRATEGY TO SECURE CYBERSPACE (2003); WHITE HOUSE, THE COMPREHENSIVE NATIONAL CYBERSECURITY INITIATIVE, available at http://www.whitehouse.gov/issues/foreign-policy/cybersecurity/national-initiative ("The activities under way to implement the recommendations of the Cyberspace Policy Review build on the Comprehensive National Cybersecurity Initiative (CNCI) launched by President George W. Bush in National Security Presidential Directive 54/Homeland Security Presidential Directive 23 (NSPD-54/HSPD-23) in January 2008. President Obama determined that the CNCI and its associated activities should evolve to become key elements of a broader, updated national U.S. cybersecurity strategy. These CNCI initiatives will play a key role in supporting the achievement of many of the key recommendations of President Obama's Cyberspace Policy Review.") Exec. Order No. 13,636 § 1, 78 Fed. Reg. 11737 (Feb. 19, 2013); WHITE HOUSE, NATIONAL SECURITY STRATEGY (2012), available at http://www.whitehouse.gov/sites/default/files/rss-viewer/national-security-strategy.pdf.

[100] *Id.*

[101] *Id.*

[102] https://fas.org/irp/offdocs/ppd/ppd-20.pdf (last visited on May 1, 2018).

[103] *Id.*

foreign relations, or economy of the United States or to the public confidence, civil liberties, or public health and safety of the American people."[104] The directive outlined five principles intended to guide the government during any cyber incident.[105] The first being a shared responsibility principle in which both the public and private sectors would work together to protect the country from "malicious cyber activity and managing cyber incidents and their consequences."[106] The directive addresses a "risk based response" in which the government would balance the need for response during a cyber incident against the harm to the country, people and civil liberties.[107] Affected entities must be ensured their rights to privacy as well as other civil liberties and therefore the federal government must safeguard the details of any cyber incident. Most importantly, the directive contends that the response to a cyber incident must balance the need for national security against the need to quickly restore and recover operations.[108]

Still, President Obama's Policy Directive is a superficial attempt at rectifying privacy concerns because the Government does not concede to the necessity of a warrant to search metadata, as required for searches under the Fourth Amendment. Instead, the current reasonable articulable suspicion standard is kept intact.[109] The Government, through FISC court documents, continually relies on the third-party doctrine in denying a reasonable expectation of privacy in metadata. However, the third-party doctrine fails to take into account the vast privacy concerns associated with modern technology. Additionally, Presidential Policy Directive 41 communicates that citizens' privacy protections are only given significance in regards to the countervailing demands

---

[104] *Id.*
[105] *Id.*
[106] *Id.*
[107] *Id.*
[108] *Id.*
[109] President Obama's Remarks, supra note 155; Presidential Policy Directive/PPD-28, Signals Intelligence Activities, THE WHITE HOUSE (Jan. 17, 2014), www.whitehouse.gov/the-press-office/2014/01/17/presidential-policy-directivesignals-intelligence-activities.

of the need for national security. This could mean that merely stating there is a national security risk could be enough to trump privacy protections as disclosing the actual national security issue could serve to jeopardize safety. Consequently, the directives are nothing more than empty promises, as it is made clear that any of the safeguards can be disregarded if they interfere with the need for national security.

V. CURRENT ATTEMPTS AT SURVEILLANCE REGULATION ONLY ADDRESS TRANSPARENCY AND DO NOT PREVENT UNWARRANTED GOVERNMENT SURVEILLANCE

On June 5, 2013, Edward Snowden revealed highly classified NSA's documents to The Guardian, a British daily newspaper, exposing FISC's secret order instructing Verizon to collect metadata from all telephone calls within the United States and abroad. Snowden disclosed that the NSA was spying on American citizens through the mass collection of "telephony metadata," with Congressional and Presidential authorization. The mass intrusion on citizens' privacy was troubling to many Americans because the NSA was not only spying on those believed to be associated with Al-Qaida but also on messages between Americans without ties to suspected terrorism. Incidental to these messages, were massive collections of sensitive and personal information that could be gathered from metadata in and of itself.

Since Edwards Snowden's disclosure of a government metadata collection program in 2013, the government has declassified some documents responsive to a request by the ACLU. But on January 17, 2018, the Justice Department said it has "withheld in full" an unspecified number of other FISA court orders that are also responsive to the request. There have also been several challenges regarding the constitutionality of Section 215 of the USA PATRIOT Act. On one hand, two U.S. District Courts have issued conflicting holdings regarding Section 215. On

the other hand, Congress reauthorized the majority of the USA PATRIOT Act's controversial provisions in 2015, and only added limited regulations on disclosure after-the-fact.

A. THE COURTS ARE RELUCTANT TO SECOND-GUESS NATIONAL SECURITY DETERMINATIONS

ACLU While the Supreme Court has yet to address the Federal Government's current cyber surveillance programs, the lower courts that have interpreted current privacy protections have shown a presumption in favor of the government when involving national security concerns. In *Klayman v. Obama*, the court found the National Security Agency's surveillance program "almost certainly" violates the Fourth Amendment.[110] The court found that the problem with this system is that people have entirely different relationships with phones today than they did when FISA regulations were first put in place.[111] Previously, call records could previously only provide police with scattered information about one's life, whereas they now "reveal an entire mosaic—a vibrant and constantly updating picture of the person's life."[112] The court further reasoned that modern society is better prepared and more willing to accept a reasonable expectation of privacy in a phone's metadata, making the collection program unconstitutional under the Fourth Amendment.[113] *Klayman* relied on the "reasonable expectation of privacy" test from *Katz* to determine that widespread data collection is unconstitutional. However, *Klayman* has since been remanded and reversed, further insolating government surveillance from judicial scrutiny.

---

[110] *Klayman v. Obama*, 957 F. Supp. 2d 1 (D.D.C. 2013)
[111] *Id.* at 36.
[112] *Id.*
[113] *Id.*

Along those lines, the court in *ACLU v. Clapper* elucidated that the sheer volume of information that the NSA can collect and store does not automatically make it a Fourth Amendment violation.[114] In *Clapper*, the ACLU and other non-profit organizations filed a lawsuit contending that by collecting metadata of the ACLU, a Verizon customer, the NSA violated their First and Fourth Amendment rights.[115] Such information could be used to identify confidential clients such as journalists, legislators, and members of the public.[116] The court held that, because Verizon users voluntarily transmitted numbers they dialed, there was no reasonable expectation of privacy in those numbers.[117] Ultimately, the court dismissed the case for lack of standing. Hence, the courts are reluctant to second guess the government when it comes to issues of national security, and will, at most, only deem such government intrusions as necessitating disclosure after-the-fact to the affected parties.

B. CONGRESS CONTINUES TO SUPPORT THE STATUS QUO BY OFFERING SOME DISCLOSURE IN EXCHANGE FOR MAINTAINING MOST SURVEILLANCE OPERATIONS

In 2015 the bipartisan USA FREEDOM Act (USAF) was signed into law just as many provisions of the USA PATRIOT Act were set to expire.[118] The USAF renewed many of those expiring provisions through 2019 as well as incorporated minor limitation on the cyber surveillance of U.S. citizens.[119] Most striking was the elimination of the NSA's bulk collection program by prohibiting bulk collection under the FISA business records provision.[120] Instead, the

---

[114] *ACLU v. Clapper*, 785 F.3d 787 (2d Cir. 2015)
[115] *Id.* at 735.
[116] *Id*.
[117] *Id*. at 752.
[118] USA FREEDOM ACT OF 2015, 161 Cong Rec S 3421
[119] *Id.*
[120] *Id.*

bulk collection program was replaced with a targeted, FISC approved call detail records program.[121] The prospective collection of call detail records is limited to 180 days.[122]

Additionally, the USAF required the government to provide additional information to Congress in its annual reporting about the use of FISA business records authority.[123] Specifically, the Act requires the government to inform Congress on compliance review matters that arise under the business records authority.[124] Another significant consequence of the legislation was a reduction in secret law. The USAF also expanded the government's obligation to supply Congress, within forty five days, FISC orders or opinions, and all related pleadings, involving a significant interpretation of law or a novel application of any provision of the Act.[125] The USAF mandates declassification of FISC opinions containing significant legal interpretations, or that a summary of an opinion be made public if declassification is not possible.[126] As a result of this provision, additional FISC opinions and orders have been declassified and made publicly available. Despite these apparently genuine attempts at reigning in data collection and surveillance, Congress continues to provide flexibility for the Federal Government to maintain covert domestic surveillance operations.

In January of 2018, the U.S. Senate voted to advance a bill that would renew Section 702 of FISA. Specifically, this bill would allow federal agencies to continue to collect vast amount of digital communications from foreigners living outside the United States via American companies like Facebook Inc., Verizon Communications Inc. and Alphabet Inc.'s Google.[127] Incidental to this

---

[121] *Id.*
[122] *Id.*
[123] *Id.*
[124] *Id.*
[125] *Id.*
[126] *Id.*
[127] Dustin Volz, Senate advances bill to renew NSA's internet surveillance program, Reuters, January 16, 2018, https://www.reuters.com/article/us-usa-congress-surveillance/senate-advances-bill-to-renew-nsas-internet-surveillance-program-idUSKBN1F528V (last visited May 1, 2018).

foreign surveillance, would be the collection of U.S. citizens' communications which can be searched without a warrant.[128] The White House, U.S. intelligence agencies and congressional Republican leaders have said the program is indispensable to national security, vital to protecting U.S. allies, and needs little or no revision.[129] The measure does add a narrow warrant requirement for cases where the FBI seeks emails related to an existing criminal investigation that has no relevance to national security.[130] This limitation gives more protections from surveillance to criminal suspects than ordinary U.S. citizens. Evidently, Congress has no plans to reign in the Federal Government's seemingly unyielding ability to conduct unwarranted surveillance on U.S. citizens as they have renewed the status quo.

CONCLUSION

Modern technology has long surpassed the privacy protections that are currently in place. Current information privacy laws do not possess the ability to grapple with the rapidly increasing collection and storage of personal information through government surveillance. The events of 9/11 forever changed the reality that was privacy as well its priority on the national agenda. The threat of global devastation, especially by fringe groups or terrorists, unfairly skews the legal balance in favor of the need for security. While it is crucial that citizens' privacy rights remain consistent with the guarantees of the Fourth Amendment, limitations may need to be placed on our freedom in order to balance the safety of the nation as a whole. Nevertheless, the current legal framework leaves privacy rights in limbo as the Federal Government continually exploits the novelty of cyberspace as a means to circumvent Fourth Amendment protections. We cannot look

[128] *Id.*
[129] *Id.*
[130] *Id.*

to the courts to remedy this situation as they are only capable of regulating surveillance off of pre-existing precedent which is not well-suited to address issues of cyber data collection. As a result, Congress must take action in order to update the existing privacy protections to adequately address the appropriate limitations on the collection of domestic cyber data.