Public Governance, Administration and Finances Law Review Vol. 9. No. 1. (2024) • 21–35.

DOI: 10.53116/pgaflr.7116

Privacy in an Age of Cybersurveillance[I]

Russell L. Weaver*

* Professor of Law, Distinguished University Scholar, Louis D. Brandeis School of Law, University of Louisville, Louisville, Kentucky, USA, e-mail: russell.weaver@louisville.edu

Submitted: 5 December, 2023 | Accepted: 23 April, 2024 | Published: 13 May, 2024.

Abstract: This article provides an update on events since Edward Snowden, an employee of a National Security Agency (NSA) contractor, stole and released thousands of classified documents in 2013, revealing that the U.S. government was engaged in a massive secret cybersurveillance operation that was amassing information about people all over the world, including U.S. citizens. In the U.S., Snowden's revelations sparked a spirited debate regarding privacy rights, and in particular whether the U.S. cybersurveillance operation was appropriate in a democratic system. This article describes the scope of the cybersuveillance program, and examines how the courts and Congress responded to the Snowden revelations, and (in particular) how U.S. society evolved in the following years.

Keywords: privacy, secrecy, FISA, terrorism, FISC, cybersurveillance, search and seizure, Bill of Rights, reasonable expectation of privacy, Fourth Amendment

1. Introduction

Americans (and perhaps the entire world) were shocked in 2013 when Edward Snowden, an employee of a National Security Agency (NSA) contractor, stole and released thousands of classified documents (Shane, 2013b; Stanglin, 2013). As the documents were published by newspapers around the world, they revealed that the U.S. was engaged in a massive secret cybersurveillance operation that was amassing information about people all over the world, including U.S. citizens (Shane, 2013b; Stanglin, 2013).

The existence of the NSA's cybersurveillance program was remarkable given U.S. history. Many in the founding generation were highly distrustful of governmental power – even a democratically-elected one (Ketcham, 1986, p. xv). Illustrative were the views of Thomas Paine (1997) who argued that: "Society in every state is a blessing, but government even in its best state is but a necessary evil; in its worst state an

[I] This paper was first presented at the Forum on Privacy and Governmental Transparency (Ludovika University of Public Service) on 8 June 2023.

intolerable one."[1] Thus, even though the Declaration of Independence flatly declared that the power to govern derives from the consent of the governed, thereby implicitly rejecting the divine right of kings and articulating the basis for what would become a representative democracy based on principles from the Enlightenment (Bailyn, 1967, pp. 16–17), including the writings of John Locke (Paine, 1997, p. 3; Doernberg, 1985, pp. 52, 57, 64–65; Konig, 2008, pp. 250, 262), Thomas Paine (Shoenberger, 2010, pp. 431–432 note 6) and Baron de Montesquieu (Adair, 1957, pp. 344–345), the Framers of the U.S. Constitution sought to create a system where governmental power was limited and constrained. For example, the Constitution (Art. I, § 3) gave Congress only limited and enumerated powers, and it included Baron de Montesquieu's doctrine of "separation of powers" (Montesquieu, 2011, pp. 151–152). Citations to Montesquieu's theories regarding separation of powers, appear in the Federalist Papers (Beeman, 2012, no. 47) and the debates at the constitutional convention (Ketcham, 1986, pp. 85, 237, 249, 253, 260, 288, 339, 360) were frequently cited and discussed in early documents (Ketcham, 1986, pp. 159–160, 163, 166–167, 240, 247, 259–260, 357), and were interspersed throughout the U.S. Constitution (Art. II, Sec. 2, Clause 2).[2]

Given the history of the U.S., Snowden's revelations sparked a spirited debate regarding privacy rights, and in particular whether the U.S. cybersurveillance operation was appropriate in a democratic system (Calmes & Wingfield, 2013; Castle, 2013; Risen & Wingfield, 2013). While government has a legitimate interest in investigating suspected terrorists, as well as in shielding certain types of information (e.g. state secrets or information vital that is potentially damaging to national security or foreign relations) from public disclosure (Calmes & Wingfield, 2013; Castle, 2013; Risen & Wingfield, 2013),[3] many questioned whether the government should be involved in such broad-based

[1] This distrust was probably rooted in a variety of considerations. First, the American Revolution was precipitated by grievances against the British Government, and in particular alleged abuses by the British monarch. See, e.g. U.S. Declaration of Independence (July 4, 1776) listing grievances against the English King (although, in fact, some of the offenses had been committed by the British Parliament rather than the King). British officials had imposed restrictions on freedom of expression; see also Weaver (2019, pp. 190–191). In addition, they had conducted aggressive searches and seizures (Weaver, 2011). However, there was a second reason to be fearful of governmental power: many in the founding generation, or their ancestors, had emigrated from Europe to the American colonies in an effort to escape religious persecution. See *Everson v. Board of Education,* 330 U.S. 1, 8–9 (1947). Some European nations had created "established" religions, required everyone to support those religions, and aggressively persecuted those who tried to practice other religions.

[2] For example, even though Congress was given the power to enact legislation, the Constitution (Art. I, Sec. 7 [3]) required the President's signature as a prerequisite to enactment into law (unless Congress overrides the President's veto or the President allows the act to become law without his signature). The President has the power to appoint "Ambassadors, other public Ministers and Consuls, Judges of the Supreme Court, and all other Officers of the United States", but he can do so only "with the Advice and Consent of the Senate" (Art. II, Sec. 2, Clause 2). Although Congress and the President jointly enact legislation, the judiciary is frequently charged with interpreting that legislation, and determining its consistency with the constitutional structure. See *Marbury v. Madison,* 5 U.S. (1 Cranch) 137 (1803).

[3] See e.g. *United States v. Nixon,* 418 U.S. 683 (1974) ordering President Nixon to release information, but noting that confidentiality regarding the President's conversations and correspondence is generally privileged, and going on to note that this privilege is "fundamental to the operation of Government and inextricably rooted in the separation of powers under the Constitution".

surveillance. As a result, when the Patriot Act,[4] which was enacted following the 9/11 attacks and provided the basis for the cybersurveillance program was up for renewal, many questioned whether it should be renewed (Hasan, 2015; Baker, 2014).

This article examines how the courts and Congress responded to the Snowden revelations, and (in particular) how U.S. society evolved in the following years.

2. Privacy and the Fourth Amendment

Although the concept of privacy is not explicitly articulated either in the U.S. Constitution or the Bill of Rights, privacy concepts played a prominent role in the formation of the U.S. governmental system. Interestingly, since the Framers of the U.S. Constitution (Art. I, § 8) had created a federal government with limited and enumerated powers, and had included separation of principles (Montesquieu, 2011, pp. 151–152),[5] they decided not to include a bill of rights in the Constitution, believing that it was unnecessary (and might even be harmful) (Bailyn, 1993, p. 808). This decision was met with vociferous opposition and threatened to derail approval of the Constitution.[6] In an effort to salvage the adoption process, a compromise was reached whereby the Constitution would be ratified "as is" (in other words, without a bill of rights), but the first Congress would be charged with proposing a list of rights.[7] As a result, the *Bill of Rights* entered the *Constitution* as the first ten amendments.

Included in the Bill of Rights were protections for a variety of rights, including protections against "unreasonable searches and seizures". The new Americans were motivated to demand these protections by abuses that occurred during the British colonial period. British officials had routinely used Writs of Assistance that allowed them to do no more than specify the object of a search, and thereby obtain a warrant allowing them

[4] USA Patriot Act of 2001, Pub. L. No. 107–56, 115 Stat. 272 (2001) codified in various sections of the United States Code. The bill was formally entitled "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA Patriot Act) Act of 2001".

[5] For example, even though Congress was given the power to enact legislation, the Constitution (Art. I, Sec. 7 [3]) required the President's signature as a prerequisite to enactment (unless Congress overrides the President's veto or the President allows the act to become law without his signature). Likewise, although Congress and the President jointly enact legislation, the judiciary is frequently charged with interpreting that legislation, and sometimes in striking it down. See *Marbury v. Madison,* 5 U.S. (1 Cranch) 137 (1803). Moreover, many powers, such as the foreign affairs power, are shared between the President and Congress. See *United States v. Curtiss Wright Export Corp.,* 299 U.S. 304 (1936). For example, the Senate is charged with ratifying treaties, which the Constitution charges the President with the power to negotiate and make (U.S. Const., Art. II, Sec. 2 [2]), but only the entire Congress can declare war (U.S. Const., Art. I, Sec. 8 [11]), and the President is integrally involved in other foreign affairs issues as well. See *United States v. Curtiss Wright Export Corp.,* 299 U.S. 304 (1936). In addition, the Framers created different terms of office for different officials so that a single election could not dramatically shift the course and direction of government (U.S. Const., Art. I, Sec. 2 [1]). See Ketcham, 1986, p. xv. "Also, mindful of colonial experience and following the arguments of Montesquieu, the idea that the legislative, executive, and judicial powers had to be 'separated,' made to 'check and balance' each other in order to prevent tyranny, gained wide acceptance."

[6] See *McDonald v. City of Chicago,* 561 U.S. 742 (2010); *Wallace v. Jaffree,* 472 U.S. 78, 92 (1985) White, J., dissenting.

[7] Ibid.

to search any place where the goods might be found (see Weaver et al., 2021, p. 64),[8] without limit as to place or duration.[9] Colonial officials had also used "general warrants" that required them only to specify an offense, and then left it to the discretion of executing officials to decide which persons should be arrested and which places should be searched.[10] These British practices infuriated the colonists.[11] In response, the Fourth Amendment provided specific privacy protections to the people. It explicitly guaranteed the American people the right to be "secure" in their persons, houses, papers and effects. In addition, it implicitly banned general warrants and writs of assistance by providing that "no warrant 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". In effect, the Fourth Amendment sought to create a balance between the societal interest in crime detection and prevention, and the individual interest in freedom from governmental intrusion as evidenced by the requirements of probable cause and particularity. Of course, the courts have subsequently created numerous exceptions to the warrant requirement, based on the idea that the Fourth Amendment only prohibits "unreasonable" searches and seizures (Weaver et al., 2021, chapter 4), but the Fourth Amendment's goal of protecting privacy remains unchanged.[12]

3. The Snowden revelations

Given the colonial history, and the Fourth Amendment protections, the Snowden revelations were striking in that they revealed a pervasive and aggressive governmental cybersurveillance program (Shane, 2013b; Stanglin, 2013). Snowden, who was stationed in Hawaii (Mazzetti & Schmidt, 2013), stole thousands of NSA documents involving the years 2007 to 2012 (Shane, 2013b; Stanglin, 2013), and fled to Hong Kong (Savage & Mazzetti, 2013). There, Snowden contacted a well-known journalist, who had written about Julian Assange and the WikiLeaks disclosures (Maass, 2013), and provided the journalist with an extensive interview and copies of thousands of classified documents disclosing the scope of the NSA surveillance program (Maass, 2013). Eventually, Snowden fled to Russia where he was granted asylum (Myers & Kramer, 2013).

Before the Snowden disclosures, while some may have suspected that the U.S. Government was spying on ordinary citizens, few envisioned the size or breadth of the surveillance operation which one commentator described as "breathtaking" (Shane, 2013b). The NSA employed 35,000 people (Shane, 2013b), had a budget of $10.8 billion

[8] See *Virginia v. Moore,* 553 U.S. 164, 168–169 (2008); *Samson v. California,* 547 U.S. 843, 858 (2006); *Atwater v. City of Lago Vista,* 532 U.S. 318, 339–340 (2001).

[9] See *Steagald v. United States,* 451 U.S. 204, 221 (1981); *Gilbert v. California,* 388 U.S. 263, 286 (1967) quoting *Boyd v. United States,* 116 U.S. 616, 625 (19).

[10] See *Virginia v. Moore,* 553 U.S. 164, 168–169 (2008); *Steagald v. United States,* 451 U.S. 204, 220 (1981); *Payton v. New York,* 445 U.S. 573 (1980).

[11] See *Carpenter v. United States,* 138 S.Ct. 2206, 2213 (2018). General warrants and writs of assistance were so "reviled" that they helped spark the Revolution; *United States v. New York Telephone Co.,* 434 U.S. 159, 180 (1977) Stewart, J., concurring in part and dissenting in part; see also *Wallace v. Jaffree,* 472 U.S. 78, 92 (1985) White, J., dissenting.

[12] See *Katz v. United States,* 389 U.S. 347 (1967).

per year (Shane, 2013b), and operated a worldwide surveillance operation (Maass, 2013). One commentator suggested that the staggering breadth of the program was motivated by the NSA's desire "not to miss anything", enhanced by a staggeringly large budget and the "near-invisibility" of the program from governmental scrutiny (Shane, 2013b).

In particular, the NSA was collecting vast amounts of electronic information, including telephonic information, phone calls, e-mails, text messages, records of credit card purchases and information from social media networks (Shane, 2013b). In addition, the NSA had hacked into foreign computers and installed software that allowed it to monitor actions on those computers (Shane, 2013b), and it had even issued a secret order to Verizon Wireless requiring that company to turn over its phone records (Maass, 2013). The NSA also developed a tool nicknamed "muscular" that it used to hack into Yahoo and Google data communication centres, thereby accessing hundreds millions of individual accounts belonging to both Americans and non-Americans (Gellman & Soltani, 2013). As a result, the NSA collected every e-mail sent through the Google or Yahoo systems or posted on the Google.doc system, involving some 1.8 million customer accounts and 182 million communication records over a single thirty-day period, including "to" and "from" e-mail information, as well as text, audio and video information (Mendoza, 2013). In addition, the U.S. Central Intelligence Agency (CIA) paid AT&T some $10 million per year for access to AT&T data files which allowed it to ask AT&T to search its database for information related to designated individuals (Angwin et al., 2015). However, because the CIA is prohibited from engaging in domestic spying on Americans, restrictions were imposed on the AT&T data collection process to protect American identities (Angwin et al., 2015). In theory, the NSA surveillance program was focused on obtaining access to communications of "foreign intelligence value", and on electronic communications that carried information pertaining to foreign intelligence targets (Mendoza, 2013). Whether this was actually true is unclear. In any event, the NSA was storing massive amounts of information for up to five years.

The NSA was even spying on foreign leaders, including the heads of allied nations such as Germany, France, Brazil, Israel and Japan (Mendoza, 2013), and had even monitored German Chancellor Angel Merkel's cellphone (Smale, 2013). In addition, the NSA had spied on United Nations Secretary General Ban Ki-moon, in advance of his visit to the White House, in order to gain access to his talking points for the meeting (Smale, 2013). When the spying on allies came to light, it produced anger and outrage with the Germans characterising the spying as "completely unacceptable (Smale, 2013) and French President Francois Hollande viewing it as "totally unacceptable" (Rubin, 2013).

Whether the NSA's surveillance operation was effective is unclear. Some argue that the NSA gathered so much information that it was simply unable to analyse or make effective use of all of the information it collected (Shane, 2013b). Indeed, some of the data involved languages that NSA analysts were not capable of reading or analysing (Shane, 2013b). The NSA defended its possession of this megadata on the basis that it gave the NSA the ability to quickly search and uncover data as needed (Shane, 2013b). One estimate suggests that as much as fifty percent of the surveillance reports delivered to President Obama each morning were based on NSA surveillance (Shane, 2013b).

4. NSA cybersurveillance and governmental accountability

Another important aspect of the NSA cybersurveillance program is that it was being conducted almost entirely in secret. Virtually no one would argue that the nation's search for terrorist activity (or, for that matter, general police operations) must be completely transparent. On the contrary, the government needs to protect its sources as well as its strategies and techniques. But, if the electorate is going to be able to control and rein in governmental authority, there must be some level of transparency so that the people are informed regarding the general scope of what the government is doing and exercise their right to rein in governmental abuses. The problem is that it managed to maintain a very high level of secrecy regarding the NSA's cybersurveillance operations so that the public was generally unaware of the size and scope of the government's surveillance operation. For example, the NSA issued National Security Letters (NSL) designed to banks, internet service providers and telephone companies (Dallal, 2018, p. 1115). These letters would order the recipient not to disclose the existence of the order to anyone, including and especially the American public and the target of the inquiries (their customers) (Dallal, 2018, p. 1116; Shane, 2013b; Stanglin, 2013). In a four year period, the NSA issued approximately 200,000 NSLs (EFF, National Security Letters).

Secrecy was further enhanced by the fact that governmental officials lied to the public regarding the nature and scope of that program. For example, President Obama assured the U.S. public that the program was not focused on ordinary U.S. citizens, but rather only on individuals who pose a terrorist threat to the United States and on communications of "foreign intelligence value" and foreign intelligence targets (Shane, 2013a; Mendoza, 2013). At one point, he boldly proclaimed: "Nobody is listening to your telephone calls" (Shane, 2013a). Likewise, the NSA declared that it was not storing private online or phone information except under limited circumstances: when it believed that the recording or transcript contained "foreign intelligence information", evidence of a possible crime, a "threat of serious harm to life or property", or shed "light on technical issues like encryption or vulnerability to cyberattacks" (Shane, 2013a). However, it soon became clear that this was not true. The NSA had established a huge data storage centre (taking advantage of the declining cost of data storage and advances in search software sophistication) (Shane & Sanger, 2013), and it was routinely collecting phone "calls and e-mails in and out of the country" (Shane, 2013a). As a result, even if Americans were not the intended targets of NSA eavesdropping, they routinely fell "into the agency's global net" (Shane, 2013a). NSA Director, James Clapper even lied to Congress about the program (The Editorial Board of the New York Times, 2014; Rosenthal, 2013; Savage & Shane, 2013). When he was directly asked whether the NSA was collecting "any type of data at all on millions or hundreds of millions of Americans", he flatly stated: "No, sir. Not wittingly" (Savage & Shane, 2013). Clapper later explained the lie by stating that it was the "most truthful" or "least untruthful" thing that he could say at the time (Rosenthal, 2013).

Although the NSA was often required to obtain search warrants, these warrants were issued by secret courts and the warrants and the court orders were classified as "secret" and

withheld from public scrutiny.[13] To the extent that individuals tried to challenge the government's cybersurveillance in court, the courts shielded the NSA against being required to divulge information.[14] In other words, it was extremely difficult for the public to ascertain the nature or scope of the operation, much less to hold governmental officials democratically accountable. Secrecy was enhanced by the fact that the Foreign Intelligence Surveillance Act (FISA) of 1978[15] provided that applications for search warrants would be governed by two courts whose orders were shielded from public view.[16]

5. Judicial restraints on the NSA's cybersurveillance program

One might have expected the federal judiciary to have restrained the cybersurveillance program, but that did not happen for a variety of reasons. In theory, the NSA's cybersurveillance was checked by the FISC (Foreign Intelligence Surveillance Court) which was given the power to oversee warrant applications. However, the FISC was a virtual rubber stamp for the NSA (Turner, 2018, pp. 995–996). The FISC heard applications for warrants *ex parte,* and it granted warrant requests in more than 99% of all cases over a thirty year period (Turner, 2018, pp. 995–996). During that time, the FISC denied only 11 warrant requests out of 33,900 applications (Turner, 2018, pp. 995–996). In 2012, the FISC did not deny any of the 1,856 applications (Turner, 2018, p. 996).

One might also have anticipated that the Fourth Amendment prohibition against unreasonable searches and seizures would have imposed a significant limitation on the NSA's cybersurveillance authority, but that did not happen either. Although the Fourth Amendment has generally provided the citizenry with substantial protections against "unreasonable searches and seizures",[17] the U.S. Supreme Court has struggled to deal with the problem of advancing technology like that being used by the NSA (see Weaver, 2011).

At the founding of the nation in the eighteenth century, the state of technology was far less advanced. At that time, since cybertechnologies did not exist, the Framers of the Fourth Amendment were concerned about actual physical searches of persons and places.[18] As a result, U.S. Supreme Court precedent tended to limit the Fourth Amendment's application to situations in which the police actually searched a person[19] or trespassed or intruded onto a "constitutionally protected area".[20] The Court's approach became problematic as technology advanced to the point that the police could reveal information without actually trespassing or intruding into a constitutionally protected area.

---

[13] See *Clapper v. Amnesty International USA,* 568 U.S. 398 (2013).

[14] Ibid.

[15] 50 U.S.C. § 1801 et seq.

[16] 50 U.S.C. § 105(a)(3) & (b).

[17] See e.g. *Arizona v. Gant,* 556 U.S. 332 (2009); *Kyllo v. United States,* 533 U.S. 27 (2001); *Florida v. Royer,* 460 U.S. 491 (1983); *Mapp v. Ohio,* 367 U.S. 643 (1961).

[18] See *Draper v. United States,* 358 U.S. 307 (1959).

[19] Ibid.

[20] See *Goldman v. United States,* 316 U.S. 129 (1942); *Olmstead v. United States,* 277 U.S. 438 (1928); *Ex Parte Jackson,* 96 U.S. 727 (1877).

The warning signs were evident by the beginning of the twentieth century. By that time, the development and use of electricity had led to technological innovations which allowed the government to invade privacy without actually entering protected spaces (see Weaver, 2011). By that time, the Court was being confronted by relatively crude technologies such as "detectaphones" (which allowed the police to hear through walls),[21] "spike mikes",[22] and wiretapping.[23] Adhering to eighteenth century principles, the Court held that the police were not engaged in a search except when they actually penetrated into a "constitutionally protected area", such as a home (e.g. in case of a spike mike which was inserted into someone's home in order to overhear conversations inside the home).[24] For the detectaphone (which simply allowed the police to capture sounds being emitted from within a room), or wiretapping (which tapped phone lines outside someone's home), the Court refused to hold that the use of such technologies to spy on citizens constituted a "search" within the meaning of the Fourth Amendment.[25]

By the early part of the twentieth century, individual justices were beginning to sound the alarm regarding the intrusive impact of new technologies on individual privacy. In *Olmstead v. United States,*[26] with a degree of prescience, a dissenting Justice Brandeis argued that the "progress of science [...] is not likely to stop with wire tapping", and may some day allow the government "without removing papers from secret drawers" to "expose to a jury the most intimate occurrences of the home".[27] Brandeis argued that rather than inquiring whether the government has intruded into a "constitutionally protected area", the courts should focus on whether government had trampled on the "indefeasible right of personal security, personal liberty and private property".[28] In *Goldman v. United States,*[29] a dissenting Justice Murphy relied on Brandeis and Warren's (1890) seminal article on privacy, to argue that the Fourth Amendment should be broadly interpreted to protect "the individual against unwarranted intrusions by others into his private affairs",[30] and that the Court should provide greater protection for individual privacy.[31]

Nearly a half a century would pass before the Court would earnestly attempt to come to grips with the intrusive possibilities of newer technologies. Finally, in its landmark decision in *Katz v. United States,*[32] the Court mapped out a completely new approach for handling advancing technologies under the Fourth Amendment. Instead of asking whether the police had intruded into a "constitutionally protected area" (which, of course, would still constitute a search within the meaning of the Fourth Amendment), the Court would

[21] See *Goldman v. United States,* 316 U.S. 129 (1942).
[22] See *Silverman v. United States,* 365 U.S. 505 (1961).
[23] See *Olmstead v. United States,* 277 U.S. 438 (1928).
[24] See *Silverman v. United States,* 365 U.S. 505 (1961).
[25] See *Olmstead v. United States,* 277 U.S. 438 (1928); *Goldman v. United States,* 316 U.S. 129 (1942).
[26] 277 U.S. 438 (1928).
[27] Ibid. 474. Brandeis, J., dissenting.
[28] Ibid. 474–475.
[29] 316 U.S. 129 (1942).
[30] Ibid. 136. Murphy, J., dissenting.
[31] Ibid. 139.
[32] 389 U.S. 347 (1967).

inquire whether the government had violated an individual's "expectation of privacy".[33] A concurring Justice Harlan essentially agreed with the Court, but argued that the expectation of privacy must be one that society recognises as "reasonable".[34] The Court ultimately adopted the Harlan formulation.

The *Katz* test seemingly expanded the Fourth Amendment's application to advancing technologies. In that case, Katz had made a phone call from a telephone booth, and the police overheard the conversation because of a listening device attached to the outside of the booth. Prior precedent enabled the prosecution to argue that there had been no intrusion into a "constitutionally protected area" because a phone booth was not a protected area (like a home). Moreover, the government had not "trespassed" into the phone booth because it had simply attached a listening device to the outside in order to capture sound waves emanating from the booth. Despite the absence of a trespass, the Court found that the government's use of the listening device involved a search because the government had violated Katz's reasonable expectation of privacy (REOP): "One who occupies [a phone booth], shuts the door behind him, and pays the toll that permits him to place a call is surely entitled to assume that the words he utters into the mouthpiece will not be broadcast to the world."[35]

After *Katz,* one might have assumed that the REOP test would be used to impose limits on technologically-based searches. In fact, the test did not provide much protection against the onslaught of technology (Weaver, 2011, pp. 1153–1227). Although the Court rendered some post-*Katz* technology decisions that were privacy protective,[36] the general thrust of the Court's REOP jurisprudence was largely unprotective (Weaver, 2011, pp. 1153–1227). The Court narrowly construed the REOP test in a way that provided little protection against electronic intrusions (Weaver, 2011, pp. 1153–1227). Indeed, in a number of cases, the Court found that individuals do not have a REOP even though a reasonable person might very well have concluded otherwise. For example, the Court held that individuals do not have a REOP in open fields (even if they are fenced and posted with "no trespassing" signs),[37] against helicopters hovering at low altitudes over their homes,[38] against surreptitious examination of garbage that they leave on the street

[33] Ibid. 351. "What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection. But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected."

[34] Ibid. 361. Harlan, J., concurring. "My understanding of the rule that has emerged from prior decisions is that there is a twofold requirement, first that a person have exhibited an actual (subjective) expectation of privacy, and, second, that the expectation be one that society is prepared to recognize as reasonable."

[35] Ibid. 352.

[36] See *Riley v. California,* 134 S. Ct. 2472 (2014). Holding that the police may not search the electronic contents of an individual's smart phone, incident to arrest, despite precedent suggesting that the police can search "closed containers" as part of such a search; *Kyllo v. United States,* 533 U.S. 27 (2001) holding that the use of Forward Looking Infrared Technology to determine the amount of heat emanating from a home (in order to determine whether the owner might be using lights to grow marijuana in his attic) constituted a "search" within the meaning of the Fourth Amendment.

[37] See e.g. *Oliver v. United States,* 466 U.S. 170 (1984). "Open fields do not provide the setting for those intimate activities that the Amendment is intended to shelter from government interference or surveillance."

[38] See e.g. *Florida v. Riley,* 448 U.S. 445 (1989); *California v. Ciraolo,* 476 U.S. 207 (1986); *Dow Chemical Co. v. United States,* 476 U.S. 227 (1986).

for the garbage collector,[39] against canine sniffs designed to uncover whether a passenger is carrying illegal drugs in a suitcase,[40] or against the use of ground tracking devices that are used to follow their movements[41] (except when the device is used to uncover information about the inside of a home[42] or the police commit a trespass in installing the device on a vehicle[43]).

Perhaps the most restrictive limitation came from the notion that there is no REOP for information that is "voluntarily conveyed to a third party".[44] In *Smith v. Maryland,*[45] the Court held that the police did not violate an individual's REOP when they installed a pen register that allowed them to mechanically record all of the phone numbers dialled by Smith. The recording was done at the phone company rather than through an intrusion into the individual's home. The Court held that an individual has no "legitimate expectation of privacy" in things that he "voluntarily turns over to third parties", including to the phone company's mechanical equipment.[46] Likewise, in *United States v. Miller,*[47] the Court held that an individual did not retain a REOP in his bank records while they were held by the bank.[48] Finally, in *Couch v. United States,*[49] the Court held that a client could not claim a REOP in documents held by his accountant.[50]

If literally applied, the "voluntarily turned over to a third party" doctrine creates a gaping hole in the Fourth Amendment, and means that the Fourth Amendment provides almost no protection against the NSA's massive surveillance operation. In a modern technologically-driven society, most information is conveyed through third parties. E-mails are routinely sent through Internet service providers (ISPs), and text messages are routinely sent through cell phone service providers like Verizon, AT&T and T-Mobile. Even phone calls are sent through phone companies. Of course, *Katz* itself involved a phone call placed through the phone company, and the Court concluded that Katz was protected by a REOP. However, in light of decisions like *Smith, Miller* and *Couch,* it is not clear that e-mails and text messages are accompanied by a REOP today.

[39] See, e.g. *California v. Greenwood,* 486 U.S. 35 (1988).
[40] See, e.g. *United States v. Place,* 462 U.S. 696 (1983).
[41] See, e.g. *United States v. Knotts,* 460 U.S. 276 (1983).
[42] See, e.g. *United States v. Karo,* 468 U.S. 705 (1984).
[43] See, e.g. *United States v. Jones,* 132 S. Ct. 945 (2012).
[44] See, e.g. *Smith v. Maryland,* 442 U.S. 735 (1979); *United States v. Miller,* 425 U.S. 435 (1976); *Couch v. United States*, 409 U.S. 322 (1973).
[45] 442 U.S. 735 (1979).
[46] Ibid. 774–775. "When he used his phone, petitioner voluntarily conveyed numerical information to the telephone company and 'exposed' that information to its equipment in the ordinary course of business. In so doing, petitioner assumed the risk that the company would reveal to police the numbers he dialed."
[47] 425 U.S. 435 (1976).
[48] Ibid. 440. Noting that Miller could not assert either ownership or possession over the records since the bank was required to keep them pursuant to its statutory obligations.
[49] 409 U.S. 322 (1973).
[50] Ibid. 335. "There can be little expectation of privacy where records are handed to an accountant, knowing that mandatory disclosure of much of the information therein is required in an income tax return."

Since these early decisions, the Court has rendered some privacy protective REOP decisions,[51] but the Court has never completely overruled the third party doctrine. However, in *Carpenter* v. *United States,*[52] the Court suggested that the third party doctrine is not without limits. In that case, the police had reason to believe that Carpenter (and others) had been involved in some robberies, they proceeded to obtain cell tower information which revealed that Carpenter was in the vicinity of the places that were robbed at the time of the robbery. The Court held that the police decision to access such information involved a search within the meaning of the Fourth Amendment.[53] In addition, although Carpenter had voluntarily conveyed information to a third party (his cell phone provider through the cell tower), the Court viewed cell phone location data as distinct from normal third party cases: "While the third-party doctrine applies to telephone numbers and bank records, it is not clear whether its logic extends to the qualitatively different category of cell-site records. When *Smith* was decided, few could have imagined a society in which a phone goes wherever its owner goes, conveying to the wireless carrier not just dialed digits, but a detailed and comprehensive record of the person's movements."[54] As a result, the Court carved out an exception to the third party doctrine: "Given the unique nature of cell phone location records, the fact that the information is held by a third party does not by itself overcome the user's claim to Fourth Amendment protection."[55] Nevertheless, the Court did not flatly overrule the third party doctrine and even suggested that special rules might apply when national security is at issue.[56]

Even if the REOP test were expanded to the point where it could be used to challenge NSA cybersurveillance, potential litigants would incur standing problems. In order to bring suit, individuals must be able to establish standing in the sense of showing that they are suffering injury. In *Clapper v. Amnesty International USA,*[57] individuals who were likely targets of surveillance sought to challenge the NSA's data collection program. However, because of the secrecy that pervaded the NSA program, plaintiffs were unable to prove that they were actual targets of the NSA program. The Court concluded that, without such proof, they could not establish standing to sue.[58] Of course, the *Clapper* decision placed most plaintiffs in an impossible situation. In order to have standing to sue, plaintiffs must be able to prove that the NSA is subjecting them to surveillance. However, the government was going to great lengths to maintain secrecy and to preclude plaintiffs for knowing whether they are subject to surveillance. In *Clapper,* plaintiffs sought to obtain the necessary information by asking that the Government be forced to reveal, through

[51] See *Riley v. California,* U.S. (2014) prohibiting the police from going through an individual's cell phone incident to an arrest; *Kyllo v. United States,* U.S. (2013) a search occurs when the police use forward looking infrared technology to determine the amount of heat coming from a house

[52] 138 S. Ct. 2206 (2018).

[53] Ibid. 2216–2218.

[54] Ibid. 2218.

[55] Ibid. 2219–2220.

[56] Ibid. 2220. "We do not disturb the application of *Smith* and *Miller* or call into question conventional surveillance techniques and tools, such as security cameras. Nor do we address other business records that might incidentally reveal location information. Further, our opinion does not consider other collection techniques involving foreign affairs or national security."

[57] 568 U.S. 398 (2013).

[58] Weaver, 2011, p. 1143. Citing *Monsanto Co. v. Geertson Seed Farms,* 130 S. Ct. 2743, 2752 (2010).

in camera proceedings, whether it was intercepting respondents' communications and what targeting procedures it was using (Weaver, 2011, p. 1149). The Court refused to require the Government to make this revelation (Weaver, 2011, p. 1149), noting that plaintiffs were required to establish standing by "pointing to specific facts", and that the Government was not required to "disprove standing by revealing details of its surveillance priorities" (Weaver, 2011, p. 1149). The net effect was that, because the government's surveillance program was super secret, plaintiffs had difficulty proving that they were under surveillance, and therefore they could not meet the case or controversy necessary to proceed with the litigation. So, judicial intervention against the NSA's cybersurveillance program was extremely limited.

6. Subsequent political developments

Perhaps the most interesting question is how the democratic process would react to the Snowden revelations. The people could demand that politicians act to rein in the NSA's cybersurveillance activities. As we shall see, the political response was rather feeble. It is not entirely clear why politicians did not react more aggressively. Perhaps politicians were concerned that terrorists might strike again, and that politicians who had acted to hamstrung the NSA's anti-terrorism activities would be blamed for the attack.

The first opportunity for a political response came when the Patriot Act, which provided the basis for the NSA's cybersurveillance program,[59] came up for renewal. The Snowden revelations provoked considerable debate regarding whether the Act should be renewed (Hasan, 2015; Baker, 2014), and Congress initially allowed the Patriot Act to expire.[60] However, Congress replaced it with the USA Freedom Act of 2015 (hereafter "Freedom Act"),[61] which imposed some restrictions on the NSA's cybersurveillance system (Steinhauer & Weisman, 2015; Shear, 2015).

Some commentators question whether the Freedom Act achieved the right balance between governmental authority and privacy.[62] The Freedom Act did a number of things. First, it placed restrictions on the ability of the NSA to gather so-called "megadata" (Carlson et al., 2016, p. 499). Previously, the NSA would collect and store large quantities of data, but (in theory at least) could only search that data when it could prove to a judge that it could link that data to terrorist activity (Berman, 2018, p. 79; Cole, 2015). Under the Freedom Act, the data would no longer be held by the government, but instead would be held by the companies that collected the data, and could only be accessed by the NSA when a judge found a reasonable suspicion of a link to terrorist activity (Cole, 2015). Second, the Freedom Act sought to increase transparency by removing the NSA's ability

[59] USA Patriot Act of 2001, Pub. L. No. 107–56, 115 Stat. 272 (2001) codified in various sections of the United States Code. The bill was formally entitled "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA Patriot Act) Act of 2001".

[60] USA Freedom Act of 2015, Pub. L. No. 114–23, 129 Stat. 268 codified at 50 U.S.C. 1801 (2016).

[61] USA Freedom Act of 2015, Pub. L. No. 114–23, 129 Stat. 268 codified at 50 U.S.C. 1801 (2016).

[62] See e.g. Cole, 2015. "In truth, the USA Freedom Act addresses only a small fraction of the NSA's dragnet surveillance operation, and will leave most of the problematic programs Edward Snowden disclosed untouched."

to prohibit the recipient of a subpoena from disclosing the existence of the subpoena (Cole, 2015). Finally, the Freedom Act provided that some opinions of the FISC should be made public (Steinhauer & Weisman, 2015; Shear, 2015). Effectively, the Act required declassification and summaries of surveillance court orders, where possible, and some reporting on the volume of surveillance requests (Cole, 2015).

Although the Freedom Act sought to rein in the NSA's cybersurveillance program, it is not clear that the Act struck the right balance. For example, although the Act prohibited the collection of megadata, the NSA could still access that data through the collecting companies based only on a showing of a "reasonable suspicion" of a link to terrorist activity (Cole, 2015). One commentator described that change as not "insignificant", and concluded that "it's hardly a radical reform" (Cole, 2015). Likewise, although FISC opinions are no longer completely withheld, it expressed concerned about how long it took to begin releasing FISC opinions, as well as the fact that they were heavily redacted, thereby reducing their value (Guariglia & Mackey, 2022).

Others have questioned the Act, suggesting that Congress could have gone farther toward transparency without compromising the first against terrorism. For example, one commentator complained that Congress deleted a provision of the Freedom Act that would have "required the government to inform us of how many Americans it collects information on each year" (Guariglia & Mackey, 2022). That commentator referred to such information as perhaps the "most important" since, "unless we are aware of the scope of what the government is doing when it spies on us, we are unlikely to be able to control it" (Guariglia & Mackey, 2022). The commentator concludes: "If we are to preserve our privacy in the digital age, we must insist on new legal constraints – including the transparency necessary to know whether the reforms we impose are working. Otherwise, the digital tracks of our lives will become increasingly transparent to a government that will be increasingly secretive about what it is doing in our name" (Guariglia & Mackey, 2022).

7. Conclusion

The Snowden revelations provoked a debate in the U.S. regarding the proper balance between the governmental (and societal) interest in rooting out terrorists, and the individual interest in privacy. Prior to the Snowden revelations, the NSA's cybersurveillance was conducted almost entirely in secret, and the American public was unaware regarding the nature and scope of the NSA's activities. The debate ultimately led to the adoption of the Freedom Act which placed some restrictions on the NSA's authority (e.g. it was no longer allowed to collect metadata), gave the public access to heavily redacted FISC opinions, and lifted a prohibition against recipients of NSL letters from discussing the existence of those orders.

Of course, the Freedom Act did not produce complete transparency regarding the nature or scope of the NSA's cybersurveillance program, and perhaps nobody thought that it would. There is a place for some level of secrecy in the fight against terrorism. Society's challenge is to find the proper balance between the fight against terrorism and the individual interest in privacy. It is not clear that the Freedom Act achieved that balance.

References

Adair, D. (1957). "That Politics May Be Reduced to a Science": David Hume, James Madison and the Tenth Federalist. *The Huntington Library Quarterly, 20*(4), 343–360. Online: https://doi.org/10.2307/3816276

Angwin, J., Savage, C., Larson, J., Moltke, H., Poitras, L. & Risen, J. (2015, August 15). *AT&T Helped U.S. Spy on Internet on a Vast Scale.* The New York Times. Online: https://shorturl.at/qN027

Bailyn, B. (1967). *The Ideological Origins of the American Revolution.* Belknap Press.

Bailyn, B. (Ed.) (1993). *The Debate on the Constitution: Federalist and Antifederalist Speeches, Articles, and Letters During the Struggle over Ratification. Part One: September 1787 – February 1788*. Library of America.

Baker, P. (2014, January 15). *Obama's Path from Critic to Overseer of Spying.* The New York Times. Online: https://shorturl.at/dfgMP

Beeman, R. (Ed.) (2012). *The Federalist Papers.* Penguin Books.

Berman, E. (2018). Digital Searches, the Fourth Amendment, and the Magistrates' Revolt. *Emory Law Journal, 68*(1), 49–94. Online: https://scholarlycommons.law.emory.edu/elj/vol68/iss1/2

Calmes, J. & Wingfield, N. (2013, December 17). *Tech Leaders and Obama Find Shared Problem: Fading Public Trust.* The New York Times. Online: https://shorturl.at/mtJL8

Carlson, J. D., Goodale, G. M., Quinlan, G. C., Suarez, S. L., Meyer, J. M., McHugh, R., Petty, K. A. & Weinstein, B. H. (2016). National Security Law. *The Year in Review. An Annual Publication of the ABA/ Section of International Law, 51,* 497–513. Online: https://shorturl.at/ostJU

Castle, S. (2013, December 25). *TV Message by Snowden Says Privacy Still Matters*. The New York Times. Online: https://shorturl.at/ghJL6

Cole, D. (2015, May 6). *Here's What's Wrong with the USA Freedom Act.* The Nation. Online: https://shorturl.at/qrL35

Dallal, R. (2018). Speak No Evil: National Security Letters, Gag Orders, and the First Amendment. *Berkeley Technology Law Journal, 33*(4), 1115–1146. Online: https://doi.org/10.15779/Z388911R16

Doernberg, D. L. (1985). "We the People": John Locke, Collective Constitutional Rights, and Standing to Challenge Government Action. *California Law Review, 73*(1), 52–118. Online: https://shorturl.at/qARSY

Electronic Frontier Foundation (EFF) (s. a.). *National Security Letters.* Online: https://shorturl.at/dehG4

Gellman, B. & Soltani, A. (2013, October 30). *NSA Infiltrates Links to Yahoo, Google Data Centers Worldwide, Snowden Documents Say.* The Washington Post. Online: https://shorturl.at/aDFJL

Guariglia, M. & Mackey, A. (2022, August 22). *Victory: Government Finally Releases Secretive Court Rulings Sought by EFF.* Electronic Frontier Foundation. Online: https://shorturl.at/mIOR8

Hasan, M. (2015, November 30). *Why I Miss George W. Bush.* The New York Times. Online: https://shorturl.at/glpT0

Ketcham, R. (Ed.) (1986). *The Anti-Federalist Papers and the Constitutional Convention Debates.* New American Library.

Konig, D. (2008). Thomas Jefferson's Armed Citizenry and the Republican Militia. *Albany Government Law Review, 1,* 250–291.

Maass, P. (2013, August 13). *How Laura Poitras Helped Snowden Spill His Secrets*. The New York Times. Online: https://shorturl.at/aoxQ2

Mazzetti, M. & Schmidt, M. S. (2013, June 9). *Ex-Worker at C.I.A. Says He Leaked Data on Surveillance.* The New York Times. Online: https://shorturl.at/qwC28

Mendoza, M. (2013, November 21). *Reagan Order Led to NSA's Broader Spying.* The Ithaca Journal.

Montesquieu, Baron de, C. (2011). *The Spirit of Laws.* Cosimo Classics.

Myers, S. L. & Kramer, A. E. (2013, August 1). *Defiant Russia Grants Snowden Year's Asylum.* The New York Times. Online: https://shorturl.at/fuzW6

Paine, T. (1997). *Common Sense.* Dover Publications.

Risen, J. & Wingfield, N. (2013, June 19). *Web's Reach Binds N.S.A. and Silicon Valley Leaders.* The New York Times. Online: https://shorturl.at/nCDMR

Rosenthal, A. (2013, October 24). *Clapper and Carney Get Slippery on Surveillance.* The New York Times. Online: https://shorturl.at/owJP4

Rubin, A. J. (2013, October 21). *French Condemn Surveillance by N.S.A.* The New York Times. Online: https://shorturl.at/dhAFG

Savage, C. & Mazzetti, M. (2013, June 10). *Cryptic Overtures and a Clandestine Meeting Gave Birth to a Blockbuster Story.* The New York Times. Online: https://shorturl.at/dgkGT

Savage, C. & Shane, S. (2013, June 17). *N.S.A. Leaker Denies Giving Secrets to China.* The New York Times. Online: https://shorturl.at/evB69

Shane, S. (2013a, June 20). *Documents Detail Restrictions on N.S.A. Surveillance.* The New York Times. Online: https://shorturl.at/yPZ23

Shane, S. (2013b, November 2). *No Morsel Too Minuscule for All-Consuming N.S.A.* The New York Times. Online: https://shorturl.at/jmyB1

Shane, S. & Sanger, D. E. (2013, June 30). *Job Title Key to Inner Access Held by Leaker.* The New York Times. Online: https://shorturl.at/cdk08

Shear, M. D. (2015, June 4). *Limits Reshape Terror Laws, and Obama's Legacy: News Analysis.* International New York Times.

Shoenberger, A. E. (2010). Connecticut Yankee in Europe's Court: An Alternative Vision of Constitutional Defamation Law to New York Times v. Sullivan? *Quinnipiac University Law Review, 28,* 431–489. Online: https://shorturl.at/ejkqQ

Smale, A. (2013, October 23). *Anger Growing among Allies on U.S. Spying.* The New York Times. Online: https://shorturl.at/AG249

Stanglin, D. (2013, July 31). *Report: Snowden Says NSA Can Tap E-Mail, Facebook Chats.* USA Today. Online: https://shorturl.at/cioDT

Steinhauer, J. & Weisman, J. (2015, June 4). *Surveillance in Place Since 2001 is Cut Back Sharply; New Legislation Curtails Sweeping Monitoring of American Phone Records.* International New York Times.

The Editorial Board of the New York Times (2014, January 1). *Edward Snowden, Whistle-Blower.* The New York Times. Online: https://shorturl.at/fBFG2

Turner, S. (2018). The Secrets of the Secret Court: An Analysis of the Missing Party and Oversight of the Foreign Intelligence Surveillance Court. *Administrative Law Review, 70*(4), 991–1019. Online: https://shorturl.at/fgtxT

Warren, S. D. & Brandeis, L. D. (1890). The Right to Privacy. *Harvard Law Review, 4*(5), 193–220. Online: https://doi.org/10.2307/1321160

Weaver, R. L. (2011). The James Otis Lecture: The Fourth Amendment, Privacy and Advancing Technology. *Mississippi Law Journal, 80,* 1131–1227.

Weaver, R. L. (2019). *From Gutenberg to the Internet. Free Speech, Advancing Technology, and the Implications for Democracy.* (2nd edition) Carolina Academic Press.

Weaver, R. L., Burkoff, J. M., Hancock, C. & Friedland, S. I. (2021). *Principles of Criminal Procedure.* (7th edition) West Academic.

This page intentionally left blank.